beroam
CCNSP

Cyberoam | Learning
academy.mybemom.com

Cyberoam Career Certification

Cyberoam Career Certification

Prepare For CCNSP Certification With The Official Companion Guide

Module 12
Managing Security solution

Cyberoam
CCNSP
Novice to Professional

Cyberoam | Learning
academy.cyberoam.com

Block login access for 1 Minutes (1-60)

Access Control

Appliance access allows limiting the Administrative access of the following appliance services from various default as well as custo

zones – LAN WAN DMZ, and VPN

Adm n Services – HTTP HTTPS Telnet, SSH

Authentication Services – Windows/Linux Client Captive portal, NTLM

Network Services – DNS P ng

Other Services – Web Proxy SSL VPN

To manage this access to devices..go to System-> Admin stration -> Appl ance Access

Default Access Control Configuration

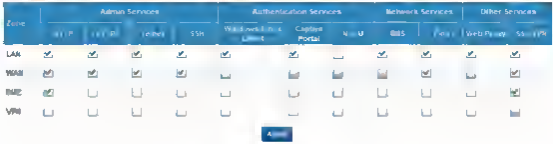
Default access conf gnation is applicable once the appliance is connected and powered up for the first t me

Admin Services – HTTP (TCP port 80) HTTPS (TCP port 443) Telnet (TCP port 23) and SSH (TCP port 22) services w ll be enable for admin strative functions in LAN zone HTTPS (TCP port 443) services will be enabled for admin strative functions in WAN zon HTTP (TCP port 80) serv ces will be enabled for administrative functions in DMZ zone

Authentication Services - Windows/Linux Client (UDP port 6060) Capt ve portal Authentication (TCP port 8090) will be enabled f User Authentication Services in LAN zone User Authentication Services are not required for any of the Administrative funct ons h required to apply user based internet surfing, bandwidth and data transfer restrictions NTLM is disabled by default for all the zones

Network Services – Ping and DNS services will be enabled for LAN zone

Other Services – Web Proxy service will be enabled for LAN zone SSL VPN (TCP port 8443) service will be enabled for LAN WA and DMZ zone



Role Based Administration

Use Profile page to create profiles for various administrator nsers Role-based administration capabilities are provided to offer greati granular access control and flex b lity

It allows an organization to separate super administrator's capabilities and assign through Profiles Profiles are a funct on of a organizat on s security needs and can be set up for spec fic purpose administrators in areas such as firewall administration netwo admin stration and logs admin stration Profiles allow to ass gn perm ssions to individual administrators depending on their role or jc need in organizat on

The profile separates appliance features into access control categories for which you can enable none read only or read wri access

For ease of use by default, appliance provides five profiles

Administrator – super admin strator with full priv leges

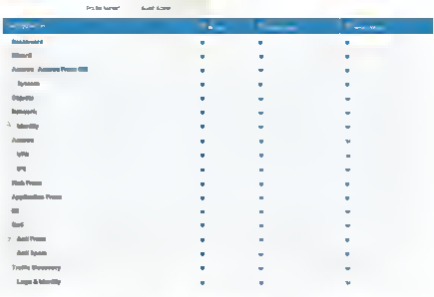
Security Admin – read-write pr vileges for all features except Profiles and Log & Reports

Audit Admin – read-write priv leges for Logs & Reports only

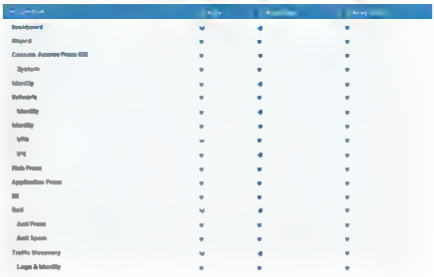
Crypto Admin – read-write privileges for Cert ficate configuration only

HAProfile – read-only privileges If HA e configured any nsm access ng Web Admin Console of Auxiliary appl ance will hav privileges as defined in HAProf le.

Shown bblow is the defaril Audit Admin profile page



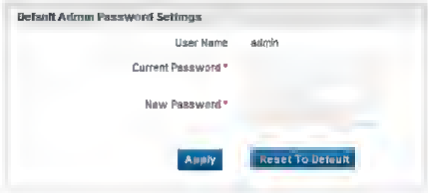
HA Profile page



Administrative Password

Appliance is shipped with one global superadmin having username & password as "admin". Both the consoles - Web Admin conso and CLI can be access with the same credentials. This administrator is always authenticated locally i e by appliance itself. W recommend changing the password for this username immediately after deployment

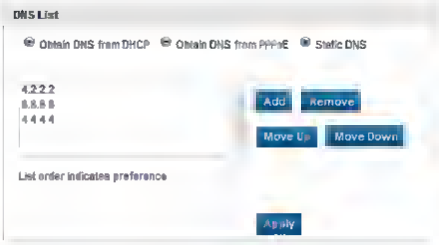
To change password, go to **System -> Administration -> Password**



DNS

Configuration

CyberoamOS allows configuring up to 3 DNS servers. The list order of the DNS in CyberoamOS specifies their preferenc
Cyberoam can be configured to get the DNS from upstream DHCP server, DHCP from PPPoE or DNS can be Static. Navigate t
Network -> DNS -> DNS to see the screen below



DNS Host Entry

DNS Host Entry allows adding DNS mapping of Domain /Host with IP Address. Adding static entry allows resolving som
Host/Domain using Cyberoam

To configure DNS go to **Network -> DNS -> DNS Host Entry**

DHCP

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP Address for the hosts on a network reducing th
Administrator's configuration task. Instead of requiring administrators to assign, track and change (when necessary) for every host o
a network, DHCP does it all automatically. Furthermore, DHCP ensures that duplicate addresses are not used.

Appliance acts as a DHCP server and assigns a unique IP Address to a host, releases the address as host leaves and re-joins th
network. Host can have different IP address every time it connects to the network. In other words, it provides a mechanism fo
allocating IP address dynamically so that addresses can be reused.

Deploying DHCP in a single segment network is easy. All DHCP messages are IP broadcast messages, and therefore all th
computers on the segment can listen and respond to these broadcasts. But things get complicated when there is more than on
subnet on the network. This is because the DHCP broadcast messages do not, by default, cross the router interfaces.

The DHCP Relay Agent allows to place DHCP clients and DHCP servers on different networks. Relay Agent makes it possible fo
DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay
Agent enables DHCP clients to obtain IP Addresses from a DHCP server on a remote subnet, or which is not located on the loca
subnet. If DHCP Relay Agent is not configured, clients would only be able to obtain IP Addresses from the DHCP server which is o
the same subnet.

Configuration

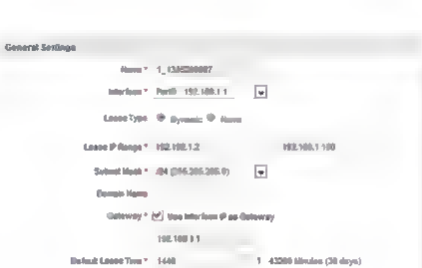
To configure DHCP go to **Network -> DHCP** > Server

Server

Each LAN and DMZ port on Cyberoam Layer 8 Firewall can be configured to act as a DHCP server. You can disable or change th
DHCP server configuration.

Static IP Lease

Dynamic IP Lease



Relay Agent

The DHCP Relay Agent allows place DHCP clients and DHCP servers on different networks Deploying DHCP in a single segme network is easy All DHCP messages are IP broadcast messages and therefore all the computers on the segment can listen ar respond to these broadcasts But things get complicated when there is more than one subnet on the network This is because th DHCP broadcast messages do not by default cross the router interfaces

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding these types of messages The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remot subnet, or which is not located on the local subnet If DHCP Relay Agent is not configured clients would only be able to obtain I addresses from the DHCP server which is on the same subnet

Note DHCP server cannot be configured when Cyberoam is deployed in bridge mode

CyberoamOS Management

Navigate to **System -> Maintenance -> Firmware** this page displays the list of available CyberoamOS versions downloaded Maximum two CyberoamOS versions are available simultaneously and one of the two CyberoamOS versions is active I e th firmware is deployed

- Upload Firmware – Administrator can upload a new firmware. Click to specify the location of the firmware image or browse to locate the file. You can simply upload the image or upload and boot from the image. The uploaded firmware can only be active after next reboot. The existing firmware will be removed and the new firmware will be available.

In case of Upload & Boot, firmware image is uploaded and upgraded to the new version, closes all sessions, restarts and displays the login page. This process may take few minutes as this process will migrate the entire configuration.

- Boot from firmware – Option to boot from the downloaded image and activate the respective firmware.
  - Boot with factory default configuration – Appliance will be rebooted and will load default configuration. Entire configuration will be lost if you choose this option.

Active – Active icon against a firmware suggests that the appliance is using that firmware.

CRLoader

Cyberoam loader (CRLoader) is very essential tool to troubleshoot as well as to recover the device from failure. This advance level debugging tool would assist the administrator by various means. It helps in loading new firmware, conducting memory test, disk test, Ethernet card test, upgrading loader, resetting console password, etc. In most of the cases where the appliance is unable to boot up completely due to some reason including fail-safe, CR loader plays an important role in device recovery as well as in troubleshooting instead of simply been replaced.

Backup – Restore

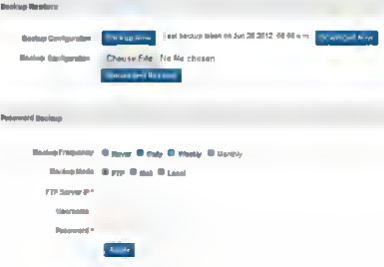
Backup is the essential part of data protection. No matter how well you treat your system, no matter how much care you take, you cannot guarantee that your data will be safe if it exists in only one place.

Backups are necessary in order to recover data from the loss due to the disk failure, accidental deletion or file corruption. There are many ways of taking backup and just as many types of media to use as well.

A CyberoamOS configuration can be backed up and restored as and when required. Backup consists of all the policies and all other user related information. To take a backup go to **Maintainance -> Backup & Restore**.

Appliance provides a facility of taking backup of only system data through scheduled automatic backup and manual backups.

Once the backup is taken, you need to upload the file for restoring the backup. Restoring data older than the current data will lead to the loss of current data.



A backup can be taken on the go or can be scheduled. The frequency of scheduling is daily, weekly and monthly respectively. The backup can be directly sent to FTP, Email or local.

Note. Backup of higher CyberoamOS version cannot be restored to lower CyberoamOS version. Backup of higher model cannot be restored to lower model appliance.

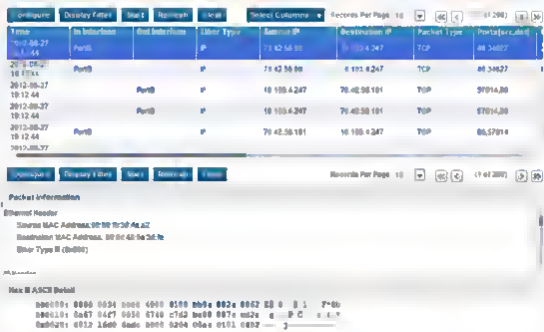
Troubleshooting

Tools

Packet capture

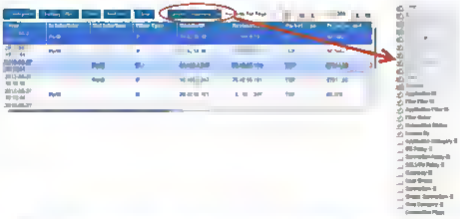
Packet capture displays packets details on the specified interface. It will provide connection details and details of the packets processed by each module packets e.g. firewall, IPS along with information like firewall rule number, user, Web and Application Filter policy number etc. This will help administrators to troubleshoot errant firewall rules.

To view packet capture tool go to **System -> Diagnostics -> Packet Capture**



Packet filter comes in very handy when very particular type of packets is to be captured

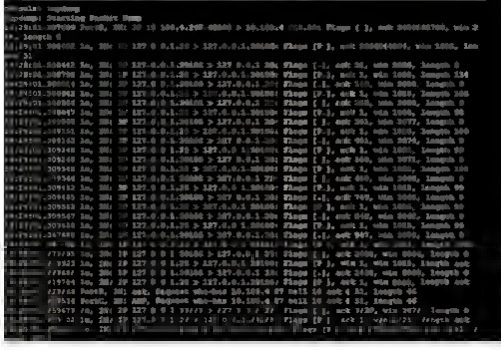
The CyberoamOS packet capture can display all the types of information as seen from the expanded select columns drop down list.



To know the precise details of the traffic the above screen can be scrolled to the right to see the below information

tcpdump

To start tcpdump, go to console option number 4 to reach the console prompt and key in tcpdump to start the tcpdump



To stop the tcpdump press ctrl + c

Understanding TCPDUMP output:

```
console> tcpdump 'port 21'
tcpdump  Starting Packet Dump
1   13:27:14.453378 PortA, IN: IP 10.120.16.100.59349 > 192.168.1.39.21: Flags [S], seq 3632672926, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
2   13:27:14.453983 PortB, OUT: IP 10.103.4.247.59349 > 192.168.1.39.21: Flags [S], seq 3632672926, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK], length 0
3   13:27:14.686967 PortB, IN: IP 192.168.1.39.21 > 10.103.4.247.59349: Flags [S.], seq 1058429879, ack 3632672927, win 5840, options [mss 1460,nop,nop,sackOK,nop,wscale 8], length 0
4   13:27:14.686378 PortA, OUT: IP 192.168.1.39.21 > 10.120.16.100.59349: Flags [S.], seq 1058429879, ack 3632672927, win 5840, options [mss 1460,nop,nop,sackOK,nop,wscale 8], length 0
5   13:27:14.686903 PortA, IN: IP 10.120.16.100.59349 > 192.168.1.39.21: Flags [.], ack 1, win 2048, length 0
6   13:27:14.687140 PortB, OUT: IP 10.103.4.247.59349 > 192.168.1.39.21: Flags [.], ack 1, win 2048, length 0
7   13:27:14.921018 PortB, IN: IP 192.168.1.39.21 > 10.103.4.247.59349: Flags [P.], ack 1, win 23, length 20
8   13:27:14.921397 PortA, OUT: IP 192.168.1.39.21 > 10.120.16.100.59349: Flags [P.], ack 1 win 23, length 20
9   13:27:15.121914 PortA, IN: IP 10.120.16.100.59349 > 192.168.1.39.21: Flags [.], ack 21, win 2043, length 0
10  13:27:15.122249 PortB, OUT: IP 10.103.4.247.59349 > 192.168.1.39.21: Flags [.], ack 21, win 2043, length 0
11  13:27:18.781053 PortA, IN: IP 10.120.16.100.59349 > 192.168.1.39.21: Flags [P.], ack 21, win 2043, length 19
12  13:27:18.781424 PortB, OUT: IP 10.103.4.247.59349 > 192.168.1.39.21: Flags [P.], ack 21 win 2043, length 19
13  13:27:19.013605 PortB, IN: IP 192.168.1.39.21 > 10.103.4.247.59349: Flags [.], ack 20, win 23, length 0
14  13:27:19.013629 PortB, IN: IP 192.168.1.39.21 > 10.103.4.247.59349: Flags [P.], ack 20, win 23, length 34
15  13:27:19.014028 PortA, OUT: IP 192.168.1.39.21 > 10.120.16.100.59349: Flags [.], ack 20
```

win 23, length 0

16 13 27 19 014257 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [P], ack 20, win 23, length 34

17 13 27 19 213374 PortA, IN IP 10 120 16 100 59349 > 192 168 1 39 21: Flags [ ], ack 55, win 2034, length 0

18 13 27 19 213734 PortB, OUT IP 10 103 4 247 59349 > 192 168 1 39 21: Flags [ ], ack 55, win 2034, length 0

19 13 27 21 429606 PortA, IN IP 10 120 16 100 59349 > 192 168 1 39 21: Flags [P], ack 55, win 2034, length 22

20 13 27 21 430018 PortB, OUT IP 10 103 4 247 59349 > 192 168 1 39 21: Flags [P], ack 55 win 2034, length 22

21 13 27 21 701511 PortB, IN IP 192 168 1 39 21 > 10 103 4 247 59349: Flags [ ], ack 42, win 23, length 0

22 13 27 21 701820 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [ ], ack 42 win 23, length 0

23 13 27 21 970660 PortB, IN IP 192 168 1 39 21 > 10 103 4 247 59349: Flags [P], ack 42, win 23, length 23

24 13 27 21 971040 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [P], ack 42, win 23, length 23

25 13 27 22 173594 PortA, IN IP 10 120 16 100 59349 > 192 168 1 39 21: Flags [ ], ack 78, win 2028, length 0

26 13 27 22 173909 PortB, OUT IP 10 103 4 247 59349 > 192 168 1 39 21: Flags [ ], ack 78, win 2028, length 0

27 13 27 23 188769 PortA, IN IP 10 120 16 100 59349 > 192 168 1 39 21: Flags [P], ack 78, win 2028, length 6

28 13 27 23 189153 PortB, OUT IP 10 103 4 247 59349 > 192 168 1 39 21: Flags [P], ack 78 win 2028, length 6

29 13 27 23 421626 PortB, IN IP 192 168 1 39 21 > 10 103 4 247 59349: Flags [ ], ack 48, win 23, length 0

30 13 27 23 421651 PortB, IN IP 192 168 1 39 21 > 10 103 4 247 59349: Flags [P], ack 48, win 23, length 14

31 13 27 23 422035 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [ ], ack 48 win 23, length 0

32 13 27 23 422266 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [P], ack 48, win 23, length 14

33 13 27 23 423114 PortB, IN IP 192 168 1 39 21 > 10 103 4 247 59349: Flags [F], seq 92, ack 48, win 23, length 0

34 13 27 23 423299 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [F], seq 92, ack 48, win 23, length 0

35 13 27 23 424184 PortA, IN IP 10 120 16 100 59349 > 192 168 1 39 21: Flags [ ], ack 93, win 2025, length 0

36 13 27 23 424419 PortB, OUT IP 10 103 4 247 59349 > 192 168 1 39 21: Flags [ ], ack 93, win 2025, length 0

37 13 27 23 426540 PortA, IN IP 10 120 16 100 59349 > 192 168 1 39 21: Flags [F], seq 48, ack 93, win 2025, length 0

38 13 27 23 426760 PortB, OUT IP 10 103 4 247 59349 > 192 168 1 39 21: Flags [F], seq 48 ack 93, win 2025, length 0

39 13 27 24 135438 PortB, IN IP 192 168 1 39 21 > 10 103 4 247 59349: Flags [ ], ack 49, win 23, length 0

40 13 27 24 135726 PortA, OUT IP 192 168 1 39 21 > 10 120 16 100 59349: Flags [ ], ack 49 win 23, length 0

1st line

Brown color shows timestamp of the packet

Green color shows the incoming interface

Purple color shows direction of packet flow i.e IN/OUT

Blue color shows source address who originates the request

Grey color shows port used by source address

Red color shows destination IP address

Orange color shows port of destination

Maroon color shows flag of particular packet.

1st line shows a new connection originated by 10.120.10.100 IP address and destined for 192.168.1.39 to access FTP services. This is first packet so flag is set to S (Sync)

2nd line Cyberoam NATs the private IP 10.120.10.100 and sends Sync request to 192.168.1.39 on behalf of it using its own public IP 10.103.4.247

3rd line This packet is the response coming back from server to Cyberoam with Ack for Sync packet. This is nothing but "Syn-Ack" packet with flag set as S

4th Line Cyberoam forwards Syn Ack packet to private IP

5th line To complete Three-way handshake, private IP sends Ack packet to Cyberoam. Flag is set to .

6th line Cyberoam forwards Ack packet to FTP server

For any tcp connection first few lines represent the Three-way Handshake which involve

Source to Destination– Sync

Destination to Source– Sync-Ack

Source to Destination—Ack

7th to 32nd lines Push packet (Data Packet) containing "P" & "." Flag

33rd and 34th line Termination of FTP connection. FTP server sends FIN packet to Cyberoam which forwards it to private IP

35th and 36th packet Private IP sends ack packet to Cyberoam which forwards it to FTP server

37th and 38th line Private IP sends FIN packet to Cyberoam which forwards it to FTP server

38th and 40th packet Server sends ack packet to Cyberoam which forwards it to private IP

Flag Information

S – Sync packet for new connection

S . – Sync packet with "ack"

P. – Push packet containing Data

-- No data information only "ack"

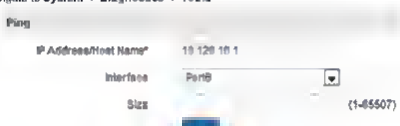
F . – FIN packet which provides information of termination of connection

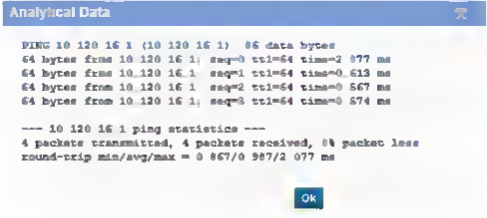
R – Reset packet. Packet which dropped in between somewhere at firewall end

Note To understand tcpdump in detail is out of scope for a CCNSP, more about tcpdump is covered in CCNSE (Cyberoam Certified Network & Security Expert). Refer training.cyberoam.com for more details on how to become CCNSE.

Ping

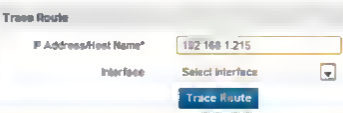
To start the ping tool navigate to **System -> Diagnostics -> Tools**

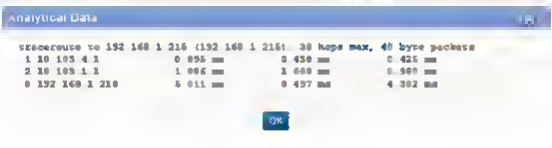



Analytical Data
PING 10 120 16 1 (10 120 16 1) 56 data bytes
64 bytes from 10 120 16 1: seq=0 ttl=64 time=2 077 ms
64 bytes from 10 120 16 1: seq=1 ttl=64 time=0 613 ms
64 bytes from 10 120 16 1: seq=2 ttl=64 time=0 567 ms
64 bytes from 10 120 16 1: seq=3 ttl=64 time=0 574 ms
--- 10 120 16 1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0 567/0 987/2 077 ms
Ok

traceroute

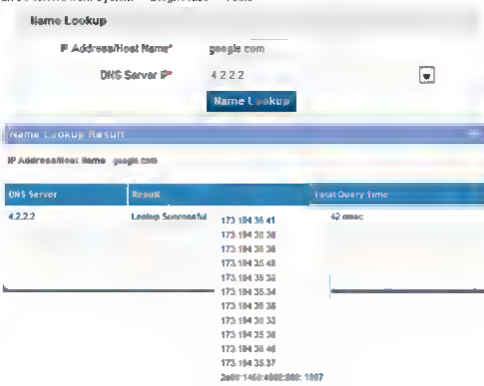
traceroute can be used to perform the full route scan on which the packet will travel. To use this tool go to System -> Diagnostics Tools





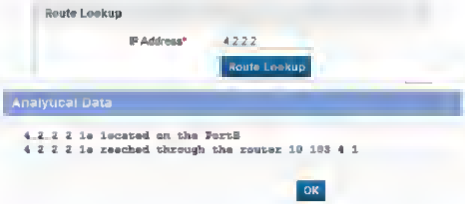
Name lookup

Name lookup can be started from System -> Diagnostics -> Tools



Route lookup

Route lookup can be started from System -> Diagnostics -> Tools



CTR (Consolidated Troubleshoot Report)

To help Support team to debug the system problems troubleshooting report can be generated which consists of the system s curre status file and log files File contains details like list of all the processes currently running on system resource usage etc. in th encrypted form

Consolidated Troubleshooting Reports is a log capture file which is required to be downloaded within the appliance This file contair the logs based on the process been triggered in debug mode The process that reqnires to be kept in debng wh le taking CTR fi depends on type of issue been face

To understand the CTR it becomes important to under the system process and how they are linked or are managed by othe process

CTR file is advanced level of troubleshooting fil meant for Cyberoam techn cal support staff ones downloaded you would require be send it across to Cyberoam technical support personnel to diagnose the logs CTR file stands to be helpful n cases where yo are unable to contact Cyberoam technical support at that very moment when issue occurred or the issue occurred is not too freque so when observed manage it to teke CTR file and send ns across at convenience

Consolidated Troubleshooting report includes System Snapshot and Log Files System Snapshot shows the system health like CP Memory Load Average whereas Log Files inclndes files the actual logs been generated before turning off the debug and th activities performed to re oreate the issue

Note To understand CTR in detail is out of scope for a CCNSP, more about CTR is covered in CCNSE (Cyberoam Certified Network & Security Expert) Refer training cyberoam com for more details on how to become CCNSE

Summary

In this module we have learnt how Cyberoam Layer 8 firewall s general administration procedures and best practices The greate part of general administration covered in this module is

Access management

Access control
DNS configuration
DHCP configuration
CyberoamOS Management
Backup – Restore
Troubleshooting tools like packet capture, tcpdump, ping, traceroute, nams lookup, route lookup
Consol data) Troubleshooting Report

Labs

Lab 61: Traffic analysis with packet capture

Packet capture displays packets details on the specified interface. It will provide connection details and details of the packe processed by each module packets e.g. firewall, IPS along with information like firewall rule number, user, Web and Application Filte policy number etc. This will help admin strators to troubleshoot disruptive firewall rules.

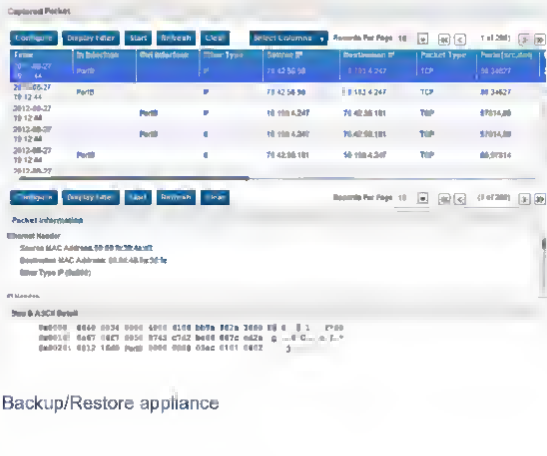
Packet capture allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network which the device is attached.

Configuration

The entire configuration is to be done from Web Admin Console. Access Web Admin Console with user having "Administrato profile.

Filter Traffic using String Based Parameters

Go to System --> Diagnostics--> Packet Capture to capture information about packets. Click the "Configure" button to configure filt settings for capturing the packets.



Lab 62: Backup/Restore appliance

Backup

The entire configuration is to be done from Web Admin console. Access Web Admin console with user having Administrato profile. Log on to the Web Admin Console of the Appliance whose backup is to be taken.

Method 1 - Automatic or Scheduled Backup

Go to System --> Maintenance --> Backup & Restore and configure backup schedule

Under "Schedule Backup" configure the backup frequency and backup mode

Frequency for Backup - Daily, Weekly and Monthly

Mode - FTP, Mail or Local (on Cyberoam).

Below is the example for Daily FTP based backup

When the backup mode selected is FTP, the filename used for the backup includes the appliance key and timestamp e.g. file name back cyberoam <appliance key> <timestamp>. This is useful when several Cyberoams are configured to send the backup to the FTP server. The appliance key in the filename acts as the differentiator

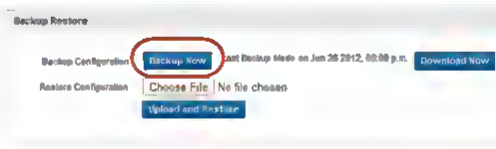
Below is the example of Weekly Mail backup

Note* - The backup is mailed with the filename as backup cyberoam with the subject line as <daily/weekly/monthly> for <appliance model for which backup is taken> <appliance key>

Method 2 Manual Backup

Step 1 Backup e Configuration

Go to **System a Maintenance --> Backup & Restore** and take the system backup till the current date



Click on **'Backup Now'** button and it creates a local copy of the Backup file on Cyberoam

A warning message will be displayed if a previous backup exists. Click on **'Take Backup**

Backup
This backup will override the backup file stored in the system. You can download backup file to your hard drive and restore it later if needed
Take Backup
Cancel

Once the backup has been taken successfully status bar will display backup successful message as.

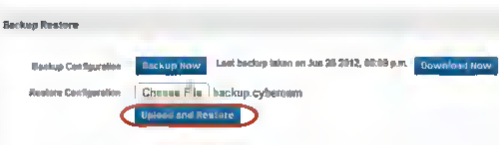
Step 2 Download Backup File

Once the backup is taken successfully Click Download Now button and save the backup file

Restore

Step 1 Upload backup file

Go to **System** » **Maintenance** » **Backup & Restore** Click Browse and specify name of the backup file to be uploaded



Click on **Upload and Restore** button to restore the uploaded data

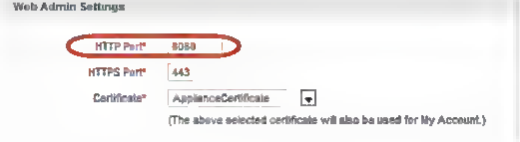
A warning message will be displayed to override the current configurations Click on **OK** button to restore This will restart appliance due to which all the users and VPN tunnels will get disconnected

Restoring this backup will override all your current configuration and will restart the appliance. Are you sure you want to restore this backup?
OK
Cancel

Once the appliance restarts Single Sign On and Clientless users will get logged in automatically while Captive Portal users will have to re-login Depending on the VPN policy VPN tunnels will get re-connected

Lab 63: Customize web admin console port

To customize web admin console port, go to System--> Administration--> Settings and key in the port you want to configure the web admin console to work on

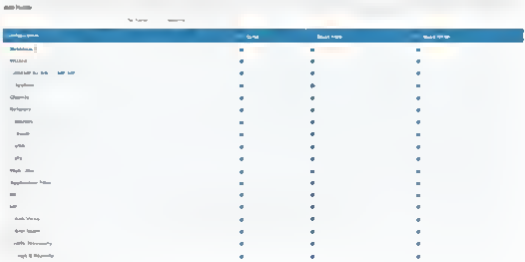


This is the end of configuration

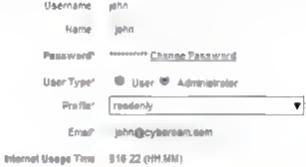
Lab 64. Give read only access of web admin console to a user

In this lab we will create a read only administrator. The purpose of this lab is to have an administrator user to look into the appliance for configuration and working but not giving the permission to modify. We will use the profile based access to achieve th functionality in this lab

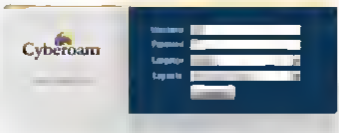
Go to System -> Administration -> Profile. Click "add" to create new profile. In this profile select the functionalities that you want th read only user to see and browse. In the "Read only" column all the modules/functionalities selected will be available to the use whom this profile is assigned. If none is selected the module will not be visible

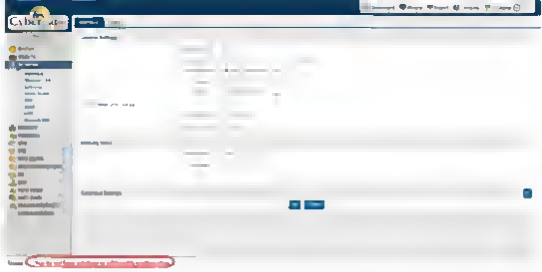


Next, save the profile go to Identity -> Users and open the user on whom you wish to apply this profile. In the profile field choos "readonly" (the profile that we just created)



From this point onwards john will be able to log into web admin console but cannot change or modify anything

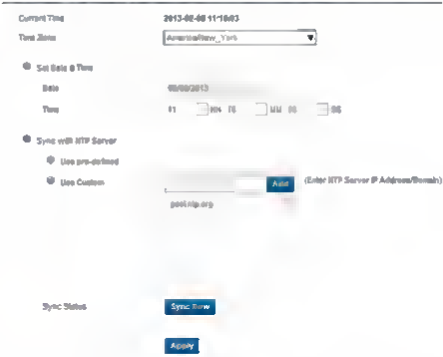




This concludes the lab

Lab 65: Configure NTP time server to synchronize clock on the appliance

To configure time on the appliance, go to System -> administration -> time. Choose your time zone. You can set the data and tim manually or sync with NTP Server. In the sync you can choose the pre-defined NTP Server or define your own. In this example w will use the worldwide NTP server pool.ntp.org



After adding the NTP server, click "Sync Now" to get the appliance in sync with the world time and click "Apply"
From now onwards, the appliance will always be in sync with the world time

Cyberoam Career Certification

Prepare For CCNSP Certification With The Official Companion Guide

Module 13

Ethical Hacks & Penetration Tests

Cyberoam

CCNSP

Cyberoam | Learning

academy.cyberoam.com

Terminologies

Before we can actually move on to what is ethical hacking and penetration testing it is essential for us to understand a few bas concepts about hacking like

Why information security is important?

In the modern era with digitization making the world a small place it is very essential to safeguard sensitive information like cred card numbers social security numbers private details of a person etc. In the case of an organization there are major examples W private data of a customer organization's own private data like design files code files marketing secrets etc.

Not only does it show that this vital for an organization to protect the information but also to take precautionary steps and b prepared for the worst case to happen Hence what is required here is that the organization be prepared for any type of attack by hacker It is rightly said that to prevent a theft think like a thief Hence to prevent a network from being hacked think like a hacke and act like a hacker In other words an Ethical hacker is required to find the flaws in this system and provide security

What are the elements of security?

We have already seen the elements of security in module 2 The elements of security are confidentiality authenticity integrity an availability

Before knowing what is hacking it is mandatory to know the following terminologies

Threat

Any event that has the potential to compromise security is a threat. Threat can be any event or action

Vulnerability

A loophole or bug in the system is known as its vulnerability Vulnerabilities can be classified into two major categories hardwar vulnerability and software vulnerability The other categories of vulnerability are based on its seriousness or severity i e Lo Medium High Critical etc.

Attack

Attack is an abstract term relating to the intention of an individual to either explore an already known vulnerability or generate a attack to find a new vulnerability

Exploit

Exploit is the defined way in which using a vulnerability the security can be compromised Exploit can be a piece of code (normal known as a tool) A common example can be given for all the terminologies above A person starts thinking about compromising a organization's security (Threat) The same person tries to break through an organization's infrastructure (Attack) He finds a wa (Vulnerability) in which attack can be done (Exploit)

Phases of hacking

Because it requires an ethical to know what a malicious hacker will do we now see what an actual hacker will do An actual hacker activity can be divided into 5 phases please note these phases are described in detail in the next section ("What is Ethic Hacking?") The five phases are -

41 Reconnaissance
42 Scanning
43 Gaining Access
44 Maintaining Access
45 Clearing Tracks

Classes of Hackers

There are four basic types of hackers or classes of hackers namely Black Hats Grey Hats White Hats and Suicide Hackers

Black hats are the bad guys also known as crackers They generally use destructive activities to take down the target with a reaso or without a reason Black hats have extraordinary computing skills

White hats are the individuals who have good hacker skills and use them to defend against the black hats These people are al known as security analysts and ethical hackers

Grey hats are the individuals who at times work as black hats and sometimes as white hats

Suicide hackers are those type of hackers whose aim is to compromise critical processes and do not care even if they were jailed fi lifetime

Hence from the above we now know that ethical hackers are the white hat community Therefore to define an ethical hacker we ca say that an ethical hacker is a person who uses their hacking skills to defend against the black hats

Cyber laws

As a learner who wants to be an ethical hacker, it is essential to know the Cyber laws prevailing in each country. To be specific every country has their own law for hackers. Hackers are dealt with severely in each country. If any hacker is found to be doing an activity that can endanger life of an individual. They can even be given a life sentence. A few acts and laws are stated below for reference.

- SPY Act
- U.S. Federal Law

Given below is the list of US Federal Laws for Cyber Crimes. More of the laws can be found on the judicial website of your country.

Posse Comitatus Act of 1879
Antitrust Laws and Section 5 of the Federal Trade Commission Act
National Institute of Standards and Technology Act
Federal Power Act
Communications Act of 1934
National Security Act of 1947
US Information and Educational Exchange Act of 1948 (Smith-Mundt Act)
State Department Basic Authorities Act of 1956
Freedom of Informal on Act (FOIA)
Omnibus Crime Control and Safe Streets Act of 1968
Racketeer Influenced and Corrupt Organizations Act (RICO)
Federal Advisory Committee Act (FACA)
Privacy Act of 1974
Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
Electronic Communications Privacy Act of 1986 (ECPA)
Department of Defense Appropriations Act, 1987
High Performance Computing Act of 1991
Communications Assistance for Law Enforcement Act of 1994 (CALEA)
Communications Decency Act of 1996
Clinger-Cohen Act (Information Technology Management Reform Act) of 1996
Identity Theft and Assumption Deterrence Act of 1998
Homeland Security Act of 2002 (HSA)
Federal Information Security Management Act of 2002 (FISMA)
Terrorism Risk Insurance Act of 2002
Cyber Security Research and Development Act, 2002
E-Government Act of 2002
Identity Theft Penalty Enhancement Act
Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

- U.K. Cyber Laws
- European Law
- Japan's Cyber Law
- Australia's Cybercrime Act
- India's Information Technology Act
- Germany's Cyber Law
- Singapore's Cyber Law
- Belgium Law
- Brazilian Law
- Canadian Laws
- France Law
- Italian Law

What is ethical hacking?

To understand "Ethical Hacking" we must first understand what is hacking and how it can be ethical. Hacking is the terminology used for an activity in which a person (hacker) gains unauthorized access to a resource which he should not be using. Unlawful hacking is the process when the hacker not only gains unauthorized access, but also modifies the content of the information in such a way that it can harm the organization. Ethical means doing a deed by abiding the principles. Hacking is no way ethical, but ethical hacking involves the hacker to use the hacking techniques to find any vulnerability in an organization's network.

Purpose of ethical Hacking

As from the above we now know that an ethical hacker is a computer and network expert who attacks the resources on behalf of its owners, seeking exploits that a malicious hacker could exploit. The primary purpose of perform ethical hacking is to test the security system. Ethical hackers use the same methods as the malicious hackers, but report problems instead of taking advantage of them.

Phases of Ethical hacking

Ethical hacking can be broadly divided into five major phases

1 Reconnaissance

Reconnaissance is the phase in which information is gathered about the victim to be attacked. Reconnaissance is a very broad term which also includes creating a foot print of the network. More about reconnaissance and Footprinting can be understood from Footprinting in the later part of this module. In Reconnaissance gathering the details with the use of computers and without the use of computers is covered. In our case we shall see Reconnaissance and Footprinting in which a computer is used to gather information about the victim

2 Scanning

Scanning involves the task to examine the information gathered from the reconnaissance

3 Gaining Access

This is the phase in which the hacker gains access to the vulnerability discovered

4 Maintaining Access

Once an access is gained, the hacker wants to keep the access for future use to launch other attacks

5 Covering Tracks

Once a hacker has been able to gain and maintain access, it becomes important for the hacker to cover the attack by adding a patch or adding another layer of security

The major phases of ethical hacking discussed above are discussed in detail in the later part of this module

Being ethical

As we have discussed about hacking and ethical hacking, we now know that an ethical hacker is the good guy, also known as White Hat. A malicious hacker is known as a Black Hat. There are some hackers who sometimes are ethical and sometimes malicious, these are categorized as Grey hats. When we talk about being ethical, we are talking of the white hats

Perform penetration test

Penetration Testing is the first job that can be done by an ethical hacker. The main function in this type of a test is to carry out an entire test on the network and check for any loop holes. If loopholes exist, the ethical hacker shall report it to the owner of the network. In this module we shall see more of ethical hacking, penetration testing in the later part of this module

Footprinting

Footprinting is a pre-attack phase which starts just after information is collected without the use of computer. We already know that during the reconnaissance phase, the hacker tries to collect as much information as possible about the target. Footprinting involves the hacker making a blueprint of the security profile defined by the organization. It is also said that the hacker spends 90% of the time collecting the information about the target and 10% to launch to the attack. Listed below are the areas which the hacker seeks during the Footprinting phase

The hacker tries to collect the following information about the target, irrespective of whether the target is on the Internet, or Intranet.

1 Domain name
2 Network Blocks
3 IP Addresses of systems that are reachable
4 Open ports
5 Running services (TCP & UDP)
6 ACLs
7 Enumerating System Users and Groups (getting SNMP info)
8 And more

The major steps involved in Footprinting are described in the paragraphs to follow

Gathering target information

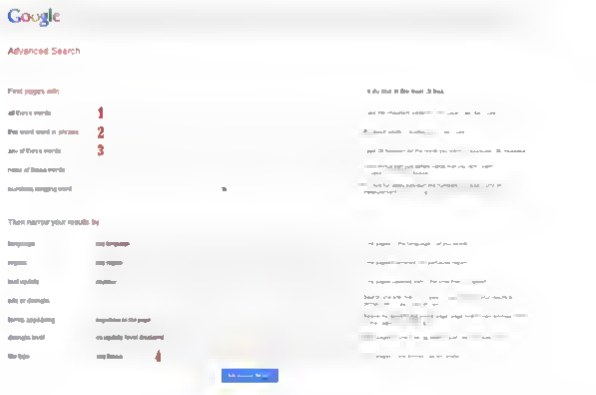
For an attack to take place, it is important that all the information about the target is gathered. It is rightly said that more time is spent over collecting the information about target than in launching the attack on the victim. The methodology adopted here includes

In this process the hacker starts from the scratch, collecting all the information like company's URL, getting an archive of the company website, getting more company information from search engines like Google, doing a people search over switchboard, yahoo, Google etc, getting the company maps from Google earth etc. The latest and proven technique to gather target information is also by scrolling job sites

- Getting the initial target information
- Locating network range
- Finding active machines in the network
- Discovering open ports
- Detecting operating systems
- Mapping the network

Using Google and other search engines

Google is by far the most used search engine in the world today. Google can be used to find information about any individual o organization. Searching on Google is comparatively easy. Google and some other popular websites can be used to get the ema address. Phone number and other details on any victim.



From the screen above, we can see that Google can be used for advanced searching. It allows the user to search the conte matching all the words (1), exact phrases (2), any of the words (3) and many more. Moreover, Google also allows to search by th type of file. The most common file types that can be searched are Word documents (doc), Shockwave Flash object (swf), Adob PDF file (pdf), Excel spreadsheet (xls), and a few more.

DNS records

In the context of a web site attack, the DNS records of the website can be searched to get the names of the registrant of the websit The DNS records also give the phone number and other contact details of the person in whose name a particular website registered. In most cases, the registrant of a website is always the administrator or the owner/CEO of the organization.

Social engineering

Social engineering is the best way to get information about any person. Social engineering involves gathering information abo target through socialization. Like for example, the attacker can send emails to a victim for friendship, or if in a case the attacke already knows the victim, they can directly approach the victim by offering some gifts and try to get the organization vital data. Soci engineering is covered again at the end of this module.

Tools

In this section, we will see the some of tools used in gathering information.

WHOIS

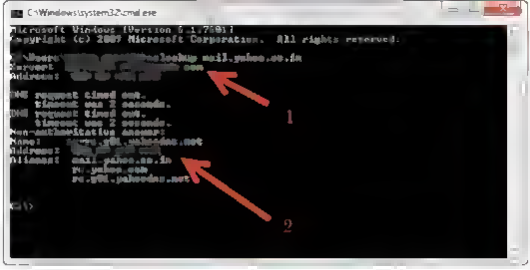
WHOIS also pronounced as *who is*, is a well known tool to find the owner information from any domain name. Lookup in WHOIS free and can be used any person over the globe. There are several websites which offer the WHOIS service like www.whois.com, www.whois.net, and many more. A sample from whois.com is shown below.

On examining in detail the WHOIS can also give details about the administrative contact of the organization as shown in the scree below

From the above screen we can clearly see how information about a target can be easily got by performing a WHOIS on the dome name

Nslookup

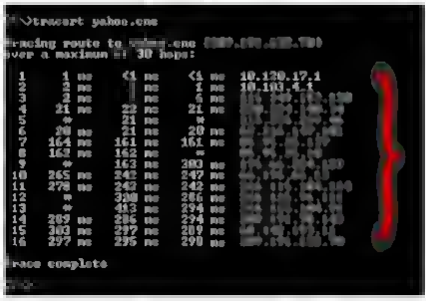
NSLOOKUP is a command line tool available with most operating systems This tool is used to obtain domain name or IP Address b querying the DNS Server NSLOOKUP means *name server lookup* In the below screens we shall be able to understand and se the NSLOOKUP tool more clearly



From the diagram above the first arrow shows the DNS server queried by the user and the second arrow shows the IP addres Name and aliases of the mail yahoo co.in server

Traceroute

Traceroute is a command line utility to find how a packet reaches from source to destination. A traceroute shows all the hops that th packet goes through during its journey from the source to destination. Traceroute can be found in most of the operating system shown below is the screen for traceroute command in windows.



The traceroute command can be issued by opening command prompt and keying tracert with the IP address or domain name a shown in the figure. From the figures the brace is the number of hops and the IP address of each hop from where the packet passed

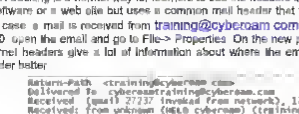
Visual route

Visual route is a similar tool to traceroute except that it is visual. The visual traceroute is a website which shows the traceroute o the world map

The screen above shows the visual traceroute from http://traceroute.monitis.com/

Email tracking

Email tracking is a normal way for learners to see the headers in an email. Any unknown email can be traced. The mail tracker is no a software or a web site but uses a common mail header that the learners need to extract and read carefully to understand. In th test case a mail is received from training@cyberoam.com to a email account. To trace this email from mail client like outloo 2010 open the email and go to File-> Properties. On the new property window that pops up we can see the Internet Headers. Th Internet headers give a lot of information about where the email is coming from. In the diagram below we shall understand th header better



From the above screen we can see that the arrow number 1 points to from (the person's email address from which the email wa sent) email address arrow number 2 points to the email address to which the email was sent. Arrow 3 points towards the subject an the other recipients of email address. More information about the email headers and email formatics can be obtained from software like email tracker pro 3d visual trace route and many other tools which are available for free by searching over Google

Other tools

There are several other tools that can be used for footprinting like ARIN Neo Trace Smart Whois eMailtracker pro Website watche Google Earth GEQ Spider HTTrack web copier Email spider, etc

Network scanning

The Scanning component is used by the attacker to gain more information about the victim From the foot printing only bas information is gathered In the scanning component the attacker will gain information about the individual like his IP addres Operating system used system architecture and services running on the victim s computer The primary objectives of scanning ar as follows

- Detecting live systems (the systems that are currently running in the network)
- Discovering which ports are active and running
- Discovering operating system being used on the victim s computer
- Discovering services running on the victim s computer
- Discovering IP address of the victim
- Discovering Vulnerability and hosts that are vulnerable
- Becoming anonymous
- Prepare and execute the attack

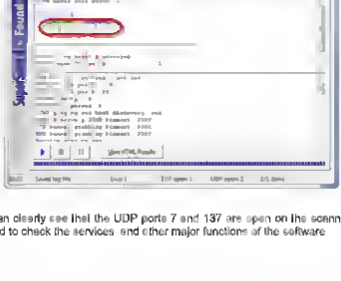
Ping sweep

A ping sweep uses ICMP protocol to determine the range of IP addresses that are live in any network We know that the ICMP use a three way handshake m which first the sender sends a SYN message to the receiver The receiver replies back with the SYN AC message and finally the sender sends a ACK message When the three way handshake is accomplished a TCP connection is established between the sender and the receiver

Tools

Pinger (Superscan)

Superscan is a port scanner, pinger and resolver Superscan is a freeware and includes other tools such as ping traceroute ht head and whois The below screen shows the functionality of the Superscan software where I found the open ports on the system



From the above screen we can clearly see that the UDP ports 7 and 137 are open on the scanned system Similarly other labe the software can be considered to check the services and other major functions of the software

Nmap

Nmap is a freeware and open source utility for exploration of a network It is designed to scan large networks faster Nmap can sca the open ports detect Operating system and many other techniques are part of the feature set The best feature of an Nmap is th It scans large number of machines in single time and it is supported by most of the operating systems

IPEye

IPEye is a TCP port scanner IPEye can provide the open TCP ports on a remote or the same host. IPEye is available for downloa as a freeware from nlsecurity com The latest version of IPEye available is 1 2

DoS, Hijacking & Viruses

DoS (Denial of Service) is an attack in which a hacker makes the system unusable or slows down the system to a significant level b overloading the resources. The goal of DoS is not to gain unauthorized access, but to prevent the users from using the services. Fi this, the attackers may

- Flood the network with heavy traffic
- Disrupt a connection between two nodes, hence affecting the communication
- Prevent an individual from accessing some particular services
- Disrupt a service to some person or system

There are several types of DoS attacks like smurf, buffer overflow, ping of death, teardrop, and SYN attack

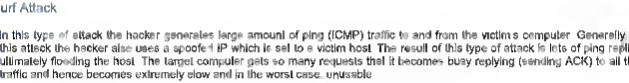
Smurf Attack

In this type of attack the hacker generates large amount of ping (ICMP) traffic to and from the victim's computer. Generally, befor this attack the hacker also uses a spoofed IP which is set to a victim host. The result of this type of attack is lots of ping replies ar ultimately flooding the host. The target computer gets so many requests that it becomes busy replying (sending ACK) to all the pir traffic and hence becomes extremely slow and in the worst case, unusable.

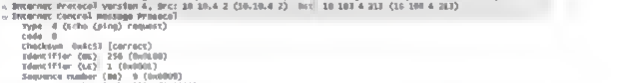
This type of attack involves three types of users

- Hacker (Originator of the attack)
- Amplifier (Actually source from where large amount of ICMP flood is generated)
- Victim (The target of attack)

Implementation of this attack: This type of attack is used by the hackers to get any website down. Since large flood is generated, the website stops responding and hence goes down. Incoming unavailable to its users. Shown below is the content of ICMP request


Frame 896: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: IntelCor_50:53:d6 (00:24:d6:50:53:d6), Dst: Abocom_a5:04:00 (00:12:0e:a5:04:00)
Internet Protocol Version 4, Src: 10.10.4.2 (10.10.4.2), Dst: 10.103.4.213 (10.103.4.213)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4c53 [correct]
Identifier (BE): 256 (0x0100)
Identifier (LE): 1 (0x0001)
Sequence number (BE): 9 (0x0009)
Sequence number (LE): 2304 (0x0900)
[Response in: 897]
Data (32 bytes)

The reply to this is


Frame 897: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Abocom_a5:04:00 (00:12:0e:a5:04:00), Dst: IntelCor_50:53:d6 (00:24:d6:50:53:d6)
Internet Protocol Version 4, Src: 10.103.4.213 (10.103.4.213), Dst: 10.10.4.2 (10.10.4.2)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x5453 [correct]
Identifier (BE): 256 (0x0100)
Identifier (LE): 1 (0x0001)
Sequence number (BE): 9 (0x0009)
Sequence number (LE): 2304 (0x0900)
[Response to: 896]
[Response time: 3.463 ms]
Data (32 bytes)

When a smurf attack is in place, the result will be lot of ping replies, like the one highlighted above.

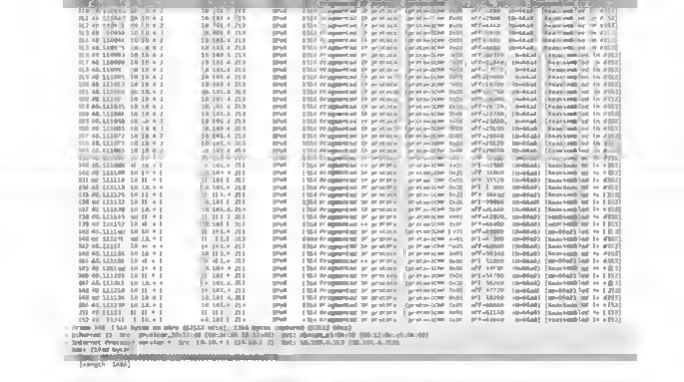
Buffer Overflow

Buffer overflow occurs when a program saves more information in the buffer than the allocated space. The attacker may replace th data in the program and hijack the program to work with attacker's code instead of process code.

The most example of a buffer overflow is sending an email whose attachment file name is more than 256 characters.

Ping of Death

In this type of attack, the attacker sends an IP packet larger than 65,536 bytes. 65,536 bytes is the maximum size allowed by an I packet. This leads to fragmentation of IP packet, in simple words, the IP packet is broken into smaller segments. In this type attacks, the operating system is unable to handle the oversized packets and hence freezes, reboots, or crashes. A sample screen shown below



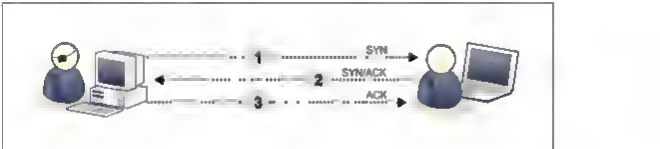
Teardrop

In the case of large IP packets, it is required that the router to handle the packet must get a fragmented packet. In this type of attac the attacker puts a confusing offset value in the later fragments and hence the receiver operating system shall not be able to arrang and get the packets. It is a UDP attack. This type of attack can crash the system. Also fragments can be overlapped to bring th system down

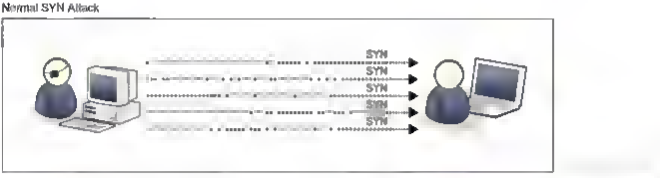
SYN Attack

In this type of attack the attacker sends multiple and non-required TCP SYN requests to a host. The host system allocates memo to each SYN and hence the host system goes slow on processing and memory available for its processes. In this type of attack th attacker actually exploits the three way handshake offered by the TCP mode of communication. The diagram below shows the SY attack with normal SYN flow

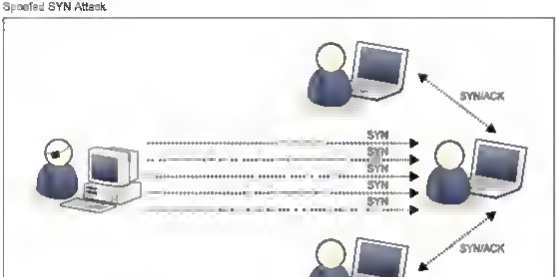
Normal SYN - SYN ACK handshake



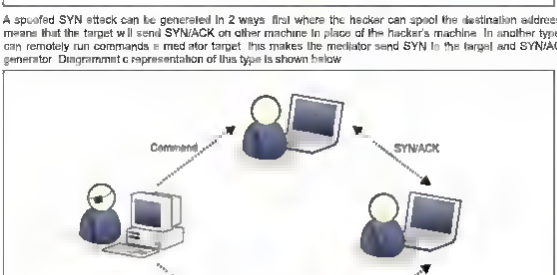
Normal SYN Attack



Spoofed SYN Attack



A spoofed SYN attack can be generated in 2 ways: first where the hacker can spoof the destination address on the packet whic means that the target will send SYN/ACK on other machine in place of the hacker's machine. In another type of attack the hacke can remotely run commands e med ator target. This makes the mediator send SYN to the target and SYN/ACK is sent back to th generator. Diagrammat c representation of this type is shown below



DDoS

DDoS (Distributed Denial of Service) according to a website.. searchsecurity.com : A distributed denial-of-service (DDoS) attack one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targete system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to th system to legitimate users.

In a typical DDoS attack, a hacker begins by exploiting a vulnerability in one computer system and making it the DDoS master. It from the master system that the intruder identifies and communicates with other systems that can be compromised. The intrude loads cracking tools available on the Internet on multiple -- sometimes thousands of -- compromised systems. With a sing command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. Th inundation of packets to the target causes a denial of service.

While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack -- th final target and as well the systems controlled by the intruder. Although the owners of co-opted computers are typically unaware th their computers have been compromised, they are nevertheless likely to suffer degradation of service and malfunction. Both owne and users of targeted sites are affected by a denial of service. Yahoo!, Buy.com, RIAA and the United States Copyright Office a among the victims of DDoS attacks. DDoS attacks can also create more widespread disruption. In October 2010, for example a massive DDoS attack took the entire country of Myanmar offline.

A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or zombie army. Both Kaspersky Labs and Symantec have identified botnets -- not spam, viruses, or worms -- as the biggest threat Internet security

Botnets

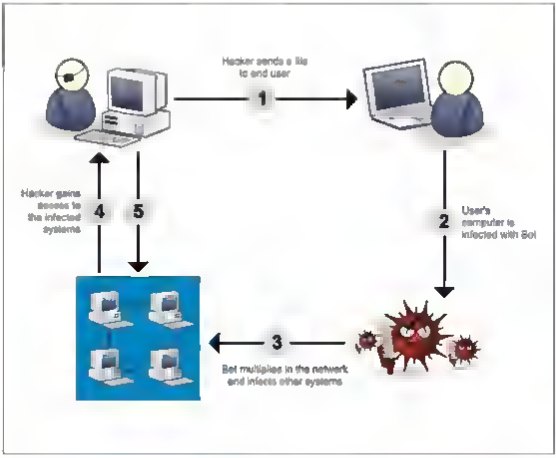
Botnets are collections of compromised computers. Each compromised computer is known as a bot, which is connected to th internet. When a computer is compromised by an attacker, the attacker often leaves a code on that computer. The primary uses botnets are

- Distributed Denial of Service Attack
- Spamming
- Sniffing Traffic
- Keylogging
- Spreading new malware
- Installing advertisement Add-ons
- Attacking chat networks
- Manipulating online polls
- Identity theft

This section describes the types of bots

- Agobot
- Phatbot
- Forbot
- XtremBot
- SDbot
- Rbot
- Urdot
- mIRC-based Bots

Functioning of Botnets



From the figure we can see that, the hacker first sends a file to the end user. Once the end user's computer is infected with the bo the bot then multiplies by looking for vulnerable systems in the network and infects them. Finally, all the systems in the netwo become infected with the bot and the hacker can gain access to all the systems in the network.

Session Hijacking

Session hijacking as defined by OWASP (The Open Web Application Security Project). The Session Hijacking attack consists of th exploitation of the web session control mechanism, which is normally managed for a session token.

Because HTTP communication uses many different TCP connections, the web server needs a method to recognize every user connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways like in the URL, in the header of the HTTP requisition as a cookie, in other parts of the header of the http request, or yet in the body of the ht

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server

The session token could be compromised in different ways. the most common are

- Predictable session token
- Session Sniffing
- Client-side attacks (XSS, malicious JaveScript Codes, Trojans, etc)
- Man-in-the-middle attack
- Man-in-the-browser attack

These attacks can be prevented by using Web Application Firewall solution like Cybernam WAF

Introduction to viruses

A virus remains the memory and dupliuates when the program containing it is run. It does not remain the memory before or after the execution of the program. A virus always operates without the knowledge or desire of the user. Viruses are written for a few specific purposes like

- Research Project
- Prank
- Vandalism
- Attack products of a company
- Distributing messages
- Financial gains
- Theft of identity
- Spying a user's computer and activity

All the viruses do not behave in a similar way or have a similar pattern of infecting the computers/network. Below we list some of the most commonly found and detected viruses

- Trojan horse

A Trojan horse appears as a useful application but starts its advertising activity after the installation. All this information is not disclosed to the user before installing the program. A Trojan horse does not duplicate itself, it damages and compromises security of the computer

- Worms

Worm is the name given to a program that duplicates itself from one drive to another or folder to folder. The worm is similar to Trojan horse can harm and compromise the security on the computer

- Bootsector Virus

This type of virus attaches itself to the boot sector of the harddisk which means every time the computer boots, it loads the virus as well. These types of viruses generally spread from external memory like CD's/DVD's or memory sticks

- Macro Virus

Macro is the term coined for large objects. A macro virus is a large virus and generally infects Word documents or Excel spreadsheets. These types of viruses are typically large in size and cannot be transferred over a network. these are spread through CD's/DVD's or removable media

- Memory resident viruses

Memory resident viruses reside in the computer's memory, mostly the RAM. They are spread as soon the computer starts. These type of viruses generally slow down the computer by using the maximum of available memory

- Rootkits

Rootkits are undetectable viruses. These types of viruses allow someone to gain control of the computer systems

Example and Working of Viruses

The most common and well known virus called "Stuxnet". It was a highly complicated virus. It was designed to malfunction the Siemens Supervisory Control And Data Acquisition (SCADA) systems which are used to monitor industrial processes. It was first discovered in June 2010

This virus targeted some industries with specific machines. It spreads via windows machines and targets the Siemens industrial software and equipment. It used to spy on the industrial system and malfunctioned the PLC (Programmable Logic Controller). PLC is a part of the machinery that is used by the industry. PLC is used for automation of electrical and mechanical processes. Given below is the working diagram taken from tofinesecurity.com

Introduction to Sniffers

Sniffing is an activity carried out by the attacker in which they intercept the traffic of the network. Sniffer is a program that captures the intercepted traffic. The primary objectives of sniffing are to capture passwords, email messages and files. The protocols that are most susceptible to sniffing are

HTTP

HTTP (Hyper Text Transfer Protocol) is more susceptible to sniffers because it sends and receives the data in non-encrypted form.

SMTP

SMTP (Simple Mail Transfer Protocol) is susceptible to sniffing because the passwords and data in SMTP are sent and received in non-encrypted form.

POP

POP (Post Office Protocol) is susceptible to sniffers because the passwords and data sent and received with POP are in a non encrypted form.

FTP

FTP (File Transfer Protocol), like all the described above, uses plain text for sending and receiving of files. The passwords and data are non-encrypted.

IMAP

IMAP (Internet Message Access Protocol) is susceptible to sniffing because it sends and receives the passwords and data in non encrypted form.

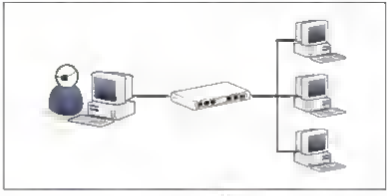
Telnet & Rlogin

Telnet and Rlogin are susceptible to sniffing of keystrokes which include the username, password, and commands.

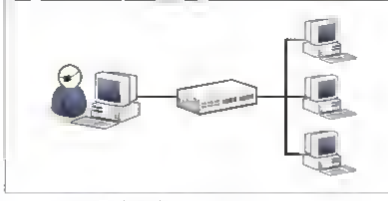
Types of sniffing

There are two types of sniffing, active and passive.

Passive sniffing: In most cases, is the only tool used for an attack. The primary reason for this is that for sniffing the attacker needs to work in a collision domain. In passive sniffing, a single collision domain is created with a hub. If a network segment is not bridged or switched, it means all the traffic can be seen by any machine in the network. However, because the traffic is not intended for any machine, the machine's network card drops it. In case of a sniffer, the sniffer software does not allow the machine's network card to drop any packet.

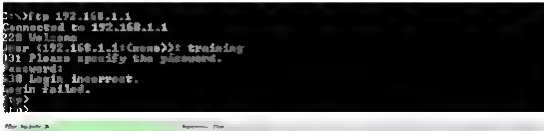


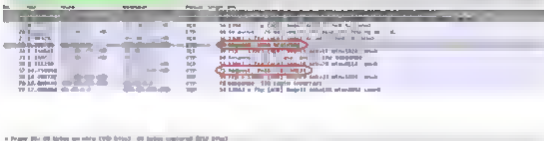
Active sniffing: is completely the opposite of passive sniffing. In active sniffing, there is no hub present and hence there is no possibility of any single collision domain. In case of switch, it creates a collision domain on each port. This means that to sniff packets in a network with switch, the attackers either needs to spoof the MAC address and sniff the packets, or can sniff the packets only for a single computer. We can say this because we know that the switch can see the MAC address of each computer connected to it. In either case, the attacker has to actively participate in the network domain to start the sniffing software.



It is evident from Sniffing that using unencrypted and clear text communication in a network is not secured. Any user in the sam network can sniff the clear text and get vital information like password etc

For an example using Wireshark tool to sniff the ftp password





Therefore it is always recommended not to enter personal information like password over non-secure protocols like HTTP. HTTP should be preferred when entering passwords. Like we see on most of the banking websites. However a note to be made here is th such websites should also be avoided where the login page is on HTTPS but other pages are on HTTP as it can expose cookie and other personal data

Social Engineering Revisited

We have already seen social engineering in the previous part of this module. In this section we shall now see social engineering detail. It is very correctly said that "There is no patch for human stupidity". Social engineering deals with the human side of breakin into a network. Having said this, the companies with authentication mechanisms, firewalls, and VPN s are still open to attacks. A lot to these resources can be innocently taken away on emails, or by answering a set of questions or over the phone. To summariz social engineering is a trick of gaining sensitive information.

Social engineering can be divided into two types: human based and computer based

Human based

Human based social engineering is when gathering of information is done by human interaction. Several examples can be take where human based social engineering can be done like

Posing as a legitimate end user who has forgotten their password.

Posing as an important user who has forgotten their password

Posing as a technical support staff that needs to access the system for maintenance

An employee's credentials can also be taken by techniques like eavesdropping. Eavesdropping, a an unauthorized techn que which the attacker may listen to conversations or reads the messages. Eavesdropping can also be in form of audio or vide Shoulder surfing is another techn que in which the attackers tries to see the keystrokes being entered by a user standing above th shoulder of a user. A binoculer is also used in some cases for shoulder surfing. Other types of human based social engineerir include dumpster diving, tailgating, and piggybacking. In dumpster diving, the attacker tries to get some valuable information from th dumps that are disposed by an organization. Tailgating is when a person wearing a fake ID card enters an organizatio n by closir following an authorized person. Piggybacking is when the attacker poses as an authorized person and asks for help. Example piggybacking can be when a fake person asks an authorized person to let him in by saying "I forgot my ID card today, can yo please open the door for me?". Reverse social engineering is another technique where an attacker creates an identity that appeal to be in the position of authority, in such case the employees ask the attacker for information rather than the other way around. Fa

reverse engineering there are several movies like catch me if you can, and the Italian job

Computer based

Computer based social engineering involves the use of computers for social engineering The most common examples of computer based social engineering is sending emails attachments in instant messaging pop-up windows spam mails

Pop up windows that suddenly come while surfing the Internet and ask the users information to log in or sign up

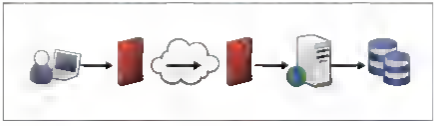
Hoax letters and chain letters are also used to get user s information

Web Hacking

In this section we will learn the essentials of hacking a web server and exploring web servers and web application vulnerabilities

How web servers work

Web servers use HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol Secure) to allow web-based clients to connect with them A clear understanding of the working principle can be seen from the figure below



Attacking a web server

A web server works on TCP port 80 (HTTP) and TCP port 443 (HTTPS) because it listens to these ports any firewall device between the web client and the web server must allow this traffic. A web server's details can be easily fetched by using the telnet tool provided in the windows command line utility

Eg

1. At the command prompt, type telnet <IP Address/domain name> 80
2. In the telnet window, type HEAD/HTTP/1 0
3. Press Enter
4. The web server banner is returned. It looks like
5. Content-Type text/html; charset=us-ascii
6. Server Microsoft-HTTPAPI/2 0
7. Date Mon 23 Jul 2012 05:05:43 GMT
8. Content-Length 326

This method is known as banner grabbing using this method the web server type and version can be identified Based on the above web server information a hacker can deface the web server Defacing of website or web server means that the hacker has exploited the vulnerabilities in the OS web server software or the website files itself

The most common attacks that enable a hacker to deface a website are

Hacking the administrator password with a brute force attack

Getting the credentials of the admin by doing MITM (Man in the middle) attack

DNS attack to redirect the users to a different web server

Doing an intrusion by telnet or SSH

Compromising an FTP or email server

Metasploit is the tool that can be used to exploit a web server vulnerability

Google hacking

Google hacking does not actually mean "hacking Google" but as a matter of fact it is referred to as using Google a powerful search technique and the engine as a hacking tool. Google can be used to locate valued targets or information like passwords. Tools like Acunetix web vulnerability scanner and Google's own operator usage for search are used for advanced searching by hackers

Eg

1. To search a string on a page "Cyberoam – securing you". Instead of writing Cyberoam securing you in the search engine you may write "Cyberoam – Securing You", including the quotes and see the search results
2. In a scenario where we wish to omit some results, like Jaguar (the car and the animal), you may write "Jaguar animal", without quotes. This search query will omit all the results of Jaguar the animal
3. To search in a specific site, for example if you want to search pages with the word training on the Cyberoam website, you can write "training site:Cyberoam.com", excluding the quotes. The results appearing will be from the Cyberoam.com website only.

Penetration Testing

Penetration testing, also commonly known as "pentest" is a technique used by ethical hackers to simulate an attack from unethical hackers on a computer or network. Pentesting a computer is more closely related to simulating attacks on an application or operating system, however our scope is network pentesting. Network pentesting involves analysis of a network for

Poor configuration

Hardware and software flaws

Operational weakness/Weakly implemented policies

The analysis is carried out with a mindset of a potential hacker who can exploit the security vulnerabilities and loop holes

Why pentest?

There are several reasons why an organization would like to perform a pentest on their network. A few as stated by the free encyclopedia "The Wikipedia" are

Determining the feasibility of a particular set of attack vectors

Identifying higher risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence

Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software

Assessing the magnitude of potential business and operational impacts of successful attacks

Testing the ability of network defenders to successfully detect and respond to the attacks

Providing evidence to support increased investments in security personnel and technology

Types of Pentesting

Pentesting approach can be divided into two major parts

White box testing

White box testing is a controlled environment or in other words when the test case is already defined. Like for example, in white box testing all the network parameters will be made available to the person who will perform penetration testing. To summarize since all the information is already made available to the person who will test the network, hence there is no need of reconnaissance in this type of testing

Black box testing

Black box testing simulates the entire hacking activity. In this type of testing, no previous knowledge about the network to be pentested is provided. To summarize, we can say that the person testing will have to start from reconnaissance phase and go up to all the other phases

In some cases where not all information is provided, is also known as "Grey box testing". To summarize all the types of testing based on informal on given, we can state

White box testing – Full disclosure

Grey box Testing –Partial disclosure

Black box testing –Blind/No Disclosure

Pentest Rationale

From what we have seen till now it s now obvious that pentest should be carried out in a captive/recreated environment and not the real world scenario For an example If a website is to be tested for penetrations it should be tested on a computer and not live over the Internet

Risks of Pentesting

Penetration testing is definitely an invaluable technique adding an extra bit to any organization s Information security program Best white box penetration testing is often done as a fully automated inexpensive process However black box penetration testing is labor intensive activity and requires expertise to minimize the risk to targeted systems

At a minimum it may slow the organization s networks response time due to network scanning and vulnerability scanning Furthermore the possibility exists that systems may be damaged in the course of penetration testing and may be rendered inoperable even though the organization benefits in knowing that the system could have been rendered inoperable by an intruder Although this risk is mitigated by the use of experienced penetration testers it can never be fully eliminated

Who should perform penetration testing?

Penetration testing abides strictly by the laws like PCI (Payment Card Industry) DSS (Data Security Standard) etc Penetration testing should not only be carried out in a controlled environment but also with the mutual agreement of the organization whose network is to be tested

The penetration testing does not require a specially certified tester but a qualified Internal resource of a qualified third party can perform this test If internal resources are being used to perform penetration tests those resources must be experienced The individuals who perform penetration testing must be organizationally separate from that domain For an example firewall administrator should not be performing penetration test on firewall

Reporting and Documentation

Before the tester performs pentest a guideline has to be followed between the organization and the tester A guideline could be in the form of a Mutual Agreement or a Non-Disclosure agreement which states the potential risk and that the tester will not use organization s private data

The documentation of each phase in pentest should be precisely mentioned There are several methodologies that can be used for penetration testing The distinction that needs to be made is how much knowledge the tester has of the system being tested Having no prior knowledge is known as "black box testing" where the tester must first identify the location of the systems before attempting any exploits Having explicit knowledge is known as "white box testing"

If it is determined that it would be beneficial for the tester to have prior knowledge there are several items required by other PCI DSS requirements that generate information that can be used Those items include

- A network diagram
- Results from a review or Self-Assessment Questionnaire (SAQ)
- Quarterly testing for presence of wireless access points
- Results from quarterly external and internal vulnerability scans
- Results from the last penetration test
- Annual identification of threats and vulnerabilities resulting in a risk assessment
- Annual review of security policies (Policies that need to be updated may identify new risks in an organization)

Documentation from all of the above should be evaluated and threats and vulnerabilities identified as part of the normal assessment processes should be considered for inclusion

Frequency

Dynamic changes in an organization s network are inevitable It is recommended that depending on the size of an organization pentest should be conducted at least once annually however the duration differs from organization to organization

Tools used

Pentesting a network using the same tools we have undergone in ethical hacking hence there are no special tools that are used to pentesting Preparation of report is a key factor while pentesting a network We shall see more in the case study to follow

Case Study

An organization XYZ wants to evaluate their network against threats and vulnerabilities This organization is opening up for pentesting for the first time and hence they are not aware what criteria and information should be given to the tester However an experienced pentester is employed at the location to conduct testing

We now see the approach of pentester from the inception.

Firstly we determine what type of pentest needs to be done viz. Black box or White box. In this case, we are looking at white bo hence the tester submits a questionnaire to the organization for gathering basic and advanced network information about th organization network.

It should be noted that the point a mutual agreement is already signed between the tester and organization. Given below is th questionnaire that was used to collect data from the organization.

The questionnaire form is at end of this module (Appendix A) and the detailed report is Appendix B.

Summary

In this module, we have learnt how ethical hacking and penetration testing can help a network administrator for possible netwo threats. As they say, better late than never". This module helps you as a network administrator to configure your network to b secure. We learnt in this module

- Ethical hacking
- Footprinting
- Network scanning
- DoS, Hijacking & Viruses
- Sniffers
- Web Hacking
- Penetration testing and its methods

Labs

Lab 66: Perform WHOIS lookup on popular websites

As seen in the module, perform WHOIS lookup using any WHOIS website and share the results with your Instructor

Lab 67: Perform NSLOOKUP on popular websites

Run the NSLOOKUP on your computer and share the results with your instructor

Lab 68: Use the TRACEROUTE tool to find the routes to a website

Use TRACEROUTE and share results with your Instructor

Lab 69: Generate a network report with all the vulnerabilities and port details

Search the web for free vulnerability scanner tools. Download and run with the permission of your instructor on the specified resourc and submit the report.

Appendix A

SCOPE DEFINITION FORM TECHNICAL SERVICES

This short assignment has been designed to obtain the preliminary information from you so that the scope and the area of focus can be effectively determined. Your input is important and appreciated. It should take approximately 15 minutes to complete this form

ABOUT ORGANIZATION

Organization

Name

Designation

Phone

Email

Nature of Business

Questionnaire (Technical)

Penetration Testing
Instructions

1 How many public / global IP's will be included in the scope? Please specify:
Please provide the details of Internet facing systems in following table

Sr No	Server / Device / Security Product	Name / Platform / Function	Number of Servers / Devices
1	Database Server		
2	Web Server		
3	Mail Server		
4	RAS Server		
5	FTP Server		
6	Proxy Server		
7	DNS Server		
8	Application Server		
9	Any other Server		
10	Firewall		
11	IDS		
12	Switches		
13	Routers		
14	Any other devices		

2 Do you host your own website / email / DNS servers? YES NO
If Yes
WWW SMTP DNS
Others Please Specify _____

3 How is your Business Application accessed by users?

Over the Internet (Client – Server) Over the Internet (Web Application) Intranet (Client Server)

Intranet (Web Application)

4 Do you want to restrict the tests to only the network, or perform comprehensive evaluation of all avenues of attack?

Restricted Comprehensive

5 Do you have network connections to suppliers of business partners? YES NO

If Yes, Please provide the information in the following table

Sr No	Server / Device / Security Product	Name / Platform / Function	Number of servers / Devices

6 Which of the following operating platforms do you use in your environment?

Windows	Linux	Solaris
BSD	HP UX	AIX
IRIX	Others Please Specify _____	

Vulnerability Assessment and Technical Audit

Please provide the network devices on which you want to conduct the Vulnerability assessment and technical audit

Sr. No	Server / Device / Security Product	Name / Platform / Function	Number of Servers / devices
1	Database Server		
2	Web Server		
3	Mail Server		
4	RAS Server		
5	FTP Server		
6	Proxy Server		
7	DNS Server		
8	Application Server		
9	Any other Server		
10	Firewall		
11	IDS		
12	Switches		
13	Routers		
14	Any other devices		

Appendix B

VULNERABILITY ASSESSMENT REPORT

DISCLAIMER

This document is strictly confidential and is intended only for the use of our client management i.e. XYZ Technologies Inc

Nothing contained in this document shall be construed as conferring by implication, estoppels, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Cyberoam Technologies Inc. or any third party. All the observations/ findings have been construed on the basis of the work carried out at XYZ during the engagement period and are based on the finding and discussion with the relevant company personnel

Cyberoam makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services and related graphics contained in this document. All such information, products, services, related graphics and other contents are provided 'as is' without warranty of any kind. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

Executive Summary

Introduction

Cyberoam Technologies is an IT company with a focus exclusively on IT security technologies as the core area of business. Cyberoam has conducted Technical Audit of critical servers and network devices of XYZ Technologies Inc. as agreed with the client. The review was conducted as per the practices followed in the industry for review of such controls

Scope of the Assignment

Following systems were audited

The goal of this audit was to determine the current security state of information systems and the efficacy of the current security infrastructure. Th assets that were assessed include
Servers
Desktops
Network Devices

The audit was conducted by the Cyberoam Technologies Consultants

Audit Summary

Positive Findings

The network is segregated into various zones using the firewall. This allows XYZ Organization to implement finer access-controls over the traffic entering and leaving the various zones.

The security infrastructure is equipped with a Cyberoam filtering device for clean traffic. This ensures that the network is safe from threats such as viruses and spam.

Findings of the Technical Audit

Server Audit Findings

The Application and Corporate servers are running on Cent OS, which are managed by developers and monitor by IT Administration team.

Currently the Application servers are accessed by Helpdesk team, IT Admin team and Development team for which there is not dedicated log management is implemented. It is recommended to have the completed audit logs based on the Roles defined in Company year.

Auditing needs to be done based on Roles, this will be useful to investigate in case of a particular incident.

There is Windows Server 2003 having the Service Pack 1 installed. The latest Service pack 4 contains fix for various critical vulnerabilities existing on Windows 2003 operating system. It is required to be installed.

Antivirus is recommended to be installed and updated on each server to protect against various viruses, worms and Malware etc.

Emergency Repair disk (ERD) is not prepared for any of the Windows server assessed. ERD always help to recover the system in case of operating system failure.

Network Devices Audit Findings

Firewall is accessible from all IP address which should be limited to the IP address. A dedicated machine can be placed inside the data center to which Network Administrators can login and manage the Cyberoam and Layer 3 switches etc. Further to strengthen the security, only Admin systems can have access to this system and this system should only be allowed to access certain ports (eg. 80, 22, 23) for network devices only.

Backup of the Firewall configuration is stored on the repository. The backup of the Firewall should be taken on external storage devices and should be kept on-site as well as off-site and should be placed in a safe. If backup is taken on Laptop, it is necessary to encrypt the file-system of the Laptop to avoid unauthorized access.

Logging on the Internet facing routers should be enabled. This helps the administrator to track any system and malicious behavior on the routers.

Change management procedures should be followed for all the systems and network devices. Change management procedures help ensures that any change made to the systems are done with prior approval from the system owner with valid reasons.

The firewall logs need to be monitored in real-time alerting the administrator of any malicious incident taking place on the network. Incident should be documented and it should be part of Incident management system.

The firewall rule sets should be accurately documented to help the administrator trace back any problem that could occur at a later stage.

Timeouts on Router, Firewall, Switches Console and VTY lines should be defined. This will reduce the chance of an unauthorized access to these devices if Admin strator leaves the console without logging out.

Detailed Audit Results

Following are the details of Overall Windows Systems at XYZ Technologies.

Windows Audit Conducted

Audit Date	20/10/2010
Owner of the system	System User's
Function	Programmers
IP Address	192.168.100.0/24
Default Gateway	192.168.100.1

Software Version

Operating System	Windows XP

Findings & Recommendations

	Findings and Recommendation	Implementation Priority
	Emergency Repair disk (ERD) is not prepared To prepare ERD follow below instructions a Click on Start à Programs à Accessories à system tools à Backup b Follow the wizard to prepare ERD	High
	There are few systems which are still not part of Domain As this is a very critical It is recommended to have all the system in Domain	High
	Power on passwords not set. We recommend setting a power on BIOS password	High
	Currently the server is accessed by Helpdesk people to restart perticular services in absence of Server Administrators However they do not log on to system since system is always logged in It is recommended to always keep the system locked and special user having appropriate rights should be created for helpdesk to maintain accountability	High
	There were no central zed patch management found server installed in We recommend having centralized patch management eg WSUS	High
	Unnecessary services like IIS messenger SMTP SNMP etc are not disabled We recommend reviewing the running services and then deciding the unnecessary services and disable them	High
	NULL session successful to desktops e g X X X X\IPC$ Refer to link http://support.microsoft.com/kb/326456	High
	Guest account on the system should be renamed to TsInternetUser account should be disabled on the system	Medium
	There were no documented procedures such as patch management change management etc found for this server We recommend documenting the procedures for patch management and change management.	Medium
	Default shares are not removed Default shares can be disabled by disabling sharing from the properties of the drives	Medium
	Default shares are not removed Default shares can be disabled by disabling sharing from the properties of the drives	Medium
	There were some critical directory shares found on the server Unnecessary directory shares should be disabled The directory shares which are in used should have proper access control list (ACL) applied and not allowing sharing to everyone	Medium
	Unnecessary services like IIS messenger SMTP SNMP etc are not disabled We recommend reviewing the running services and then deciding the unnecessary services and disable them	Medium
	Administrator account has not been renamed Rename the Administrator account to some other name Create different accounts if the server is administered by more than one person to have proper accountab lity	Medium
	Everyone group was found in the security tab of drive properties Replace the "Everyone" Group with "Authenticated Users" on file shares/security Try to have a tight shares/security standard to protect information	Medium

Cyberoam Firewall

Audit Date	20/10/2010
Owner of the system	Security Administrator / IT Administrator
IP Address	192.168.100.1
Function	Firewall Perimeter Protection
Cyberoam Model	Cyberoam 100iA

Questions	Findings Yes	Findings No	Comments	Implementation Priority
Baselines and Procedures Has a firewall baseline and the procedures relating to the firewall been documented?	o	y		A baseline for the firewall helps the organization to implement a security level that is consistent across the organization Documented procedures relating to backup monitoring and incidence response of the firewall makes the activity person independent.
Identification & Authentication Is the firewall being managed by third party personnel or by the organization itself? If managed by third party personnel has a NDA being signed?	ý	o		Third Party personnel managing the firewall of an organization need to sign a NDA with the latter
Are all administrators authenticated using individual accounts before granting access to the firewall's administration interface?	o	ý		Maintaining individual accounts for each administrator helps implement accountability for any malicious activity undertaken intentionally or unintentionally
What is the procedure for the			Since only one user account exists on the	Procedures should address the creation

creation of users/administrators on the firewall?			firewall there is no procedure currently implemented	as well as the deletion of the user accounts created on the firewall
Are all administrator accounts assigned the lowest privilege level that allows them to perform their duties?	e	e	Not applicable	Administrators should be assigned the lowest privilege level that allows them to perform their job
How often is the firewall configurat on reviewed for presence of unauthorized accounts?			Since the firewall does not have any accounts reviewing the configuration for the same does not apply nonetheless the configurat on file should be reviewed to check for other parameters such as access-lists	Unauthorized accounts pose a serious threat to the overall security posture of the organization A regular review based on company policy helps el m nate the risk posed by unauthorized accounts
Configuration Is the firewall configured to be able to protect the network against denial of service attacks such as Ping of Death TCP SYN floods etc	ý	o		
Is any sort of Ingress/Egress Filtering configured?	ý	o		
Does the f rewall use the latest version of the firewall software w th all securi ty-related patches applied?	e	y	Firewall is running Vers on 8 00 Build 78 Cyberoam has released Vers on 10 which is required to be upgraded	
How often is the firewall configurat on rule sets tested in the form of a PT/VA? Last test done on			The VA and PT have never been done earlier	As part of the network pol cy periodic assessment of the rule sets in the form of a VA/PT should be conducted Rule sets should be tested every 6 months to a year depending on the number of changes made to the configuration file
Are the firewall administrators registered with the vendors vulnerabi ty mailing list to keep themselves updated with the latest security patches?	o	ý	Cyberoam is required to do it	Firewall administrators should subscribe to vulnerability mailing l st pertain ng to the f rewall in order to be aware of the latest vulnerabilities affecting their product
Does the firewall perform anti-virus scanning and content security checking of all inbound packets for HTTP FTP and SMTP?	ý	e		
How is the performance of the firewall monitored? (memory CPU)	ý	e	Cyberoam has a built in monitoring system	As part of the capacity management procedure period c reviews of the key parameters such as memory CPU should be mentored to address current and future needs
Are any VPN s configured on the firewall?	ý	e		
Auditing and Admin stration Are log recipient hosts identified and configured?	e	ý	There is logging host defined but it does not exist	Logging can help to track the incident
Is the security of the logs on the host maintained through local operating system settings?	e	e	Not Applicable	Local Operat ng system settings protect the logs from unauthorized access.
How often are the logs reviewed? Is a report sent to the upper management about the status of the report?	n	e	Not Applicable	The review of logs should be documented and to send to the manager for review
Is logging timestamp enabled?	ý	o		Including timestamps in messages will allow you to trace network attacks more credibly
Is the time synchronized with a NTP Server? Are logs reviewed/ monitored regularly?	ý	o		
Periodicity (Real Time/ Daily/ Weekly/ Monthly/ _____	n	ý	Logs are not reviewed	
Are the logs backed up? How often s the backup taken? What is the retention period of the logs?	ý	e	15 Days	
Is the firewall configuration data backed up weekly and whenever configuration changes occur?	ý	o	The firewall configuration s backed up whenever a change s made to the firewall The backup of configuration s stored on the Laptop and on repository server	Firewall configuration should be backed up according to the firewall pol cy (whenever configuration changes take place)
Where is the configuration data backup stored?				The configuration files should be stored either on tapes or a file server Logical/Physical controls need to be implemented on the file server to prevent unauthorized access
Is the firewall configuration well documented?	e	ý		Firewall configuration should be well documented
Is a login banner defined when accessing the firewall?	n	ý		Login banner should be defined on the firewall This can aid in prosecution in some jurisdictions and also serves as a preventive measure in unauthorized access
Is the firewall configured to alarm the administrator of a potential attack or system failure?	ý	e		
What is the procedure followed upon			No formal procedure has been documented	A documented Incident Management Procedure should be

#detection of a particular incident?		for incident reporting on the firewall	available for alerts detected by the firewall
Is two-factor authentication used for in-band (telnet) management of the firewall?	o	ý	
Is in-band management restricted to a limited number of IP addresses?	o	ý	It should always be restricted and limited
Are all in-band management access to all firewalls via SSH?	ý	o	Yes the firewall management is done over ssh and HTTPS
Is a local password assigned to the telnet or ssh process?	ý	o	All management communication between the management hosts and the firewall should be encrypted The password should be stored in a manner consistent with your site's security policy
Is SNMP used to manage the firewall? If no is the service disabled?	o	ý	If the SNMP service is not used to mange the firewall, it should be explicitly disabled
Is a timeout defined for idle sessions?	ý	o	
Configuration Change Management			
Is there a documented change management procedure for any changes done on the firewall?	ý	o	Since the application software change management document addresses software change management procedures it should be expanded to include networking devices such as the firewall too
Management & Monitoring			
Is the firewall configuration reviewed periodically?			
Review Period: Monthly/ Quarterly / _____	o	ý	
Last review done on _____			
Is the firewall configuration (hard copy) stored in a secured location?	o	ý	Firewall configuration hard copies are not maintained
Is the firewall administrator details (matrix) document updated?	o	ý	Not applicable since there is no separate account for each administrator
Last date of update _____			
Failover / Redundancy			
Is the firewall configured for proper recovery from failure or interruption?	o	ý	HA should configured as this is a critical device
What is the procedure to be followed if the firewall fails?			
Is the hot standby firewall in sync with active firewall configuration and software updates?	o	ý	
Is the hot standby/recovery procedures of the firewall periodically tested?			
Periodicity: Monthly/ Quarterly/ _____	o	ý	
Date of last test performed _____			

Findings & Recommendations

S. No	Finding	Recommendation	Priority
1	The configuration file should be reviewed periodically to check for its accuracy. For e.g. to check the requirement and accuracy of access-lists		High
2	Logging is enabled by defining logging host, however this host is not connected to the network always		High
3	Logs should be stored on logging host which is hardened enough		
4	Firewall is accessible from the whole network. A dedicated machine can be placed inside the data center to which Admin can login and manage the Cyberoam and Layer 3 switches etc. Further to strengthsn the security only Admin system is can have access to this system and this system should only be allowed to access certain ports (eg. #0, 22, 23) on network devices only		High
5	The review of logs should be documented and send to the manager for review		High
6	Logs of the firewall should be backed up and retained. This will prove useful if old logs have to be looked into to investigate a particular incident.		Medium
7	Log retention time period should be defined		
8	As part of the ongoing management procedure, periodic reviews of the key parameters such as memory, CPU should be monitored on the firewall to address current and future needs		Medium
9	Log in banner should be defined on the firewall. This can aid in prosecution in some jurisdictions and also serves as a preventive measure to unauthorized access		Medium
10	A documented Incident Management Procedure should be available for alerts detected by the firewall.		Medium
11	Firewall baseline and the procedures related to the firewall should be documented		Medium
12	Procedures should address the creation as well as the deletion of the user accounts created on the firewall		Low
13	Firewall configuration should be well documented		Low

Layer 3 Switch

Audit Date	20/10/2010
Owner of the system	Network Administrator / Helpdesk
IP Address	192.168.100.2
Function	Computer Networking
Switch Model	Cisco 3850

Questions	Flag Yes	Flag No	Comments	Standard Date
Disable Unneeded Services				
Is TCP small servers, UDP small servers and the finger service disabled on the switch? (applicable before Cisco IOS 11.3)	o	o	Not Applicable	These services are not required on a production switch and hence need to be disabled Switch(config)#no service tcp-small-servers Switch(config)#no service udp-small servers Switch(config)#no service finger
Is Bootp server disabled on the switches?	ý	o	Although these services are disabled by default on recent versions of the switch there is no harm in having the bootp service explicitly disabled using the command as shown under the best practice column	The feature should be disabled on the switch The following command is used to disable the service Switch(config)#no ip bootp server
Is Configuration Autoload disabled on the switch?	o	ý		Informat on passed through the network when configuration autoload is enabled is clear text and can be processed by unauthorized users The following can be done to disable this feature Switch(config)#no service config Switch(config)#no boot host Switch(config)#no boot network Switch(config)#no boot system
Is PAD (packet assembler/disassembler) enabled on the switch?	ý	o		The following can be done to disable this feature Switch(config)#no service pad
Is directed broadcast disabled on all interfaces?	o	ý		This feature should be disabled on the switch The following command is used to disable the service Switch(config-if)#no ip directed-broadcast
Is Proxy ARP disabled on the switch?	o	ý		This feature should be disabled on the switch The following command is used to disable the service Switch(config-if)#no ip proxy-arp
Is Flow Control turned off?	o	ý		To prevent misuse of the Flow control feature the same should be disabled Switch (config-if)# flowcontrol receive off
If UDLD (Unidirectional Link Detection) is enabled is UDLD disabled globally and on each and every interface?	o	ý		To prevent misuse of the UDLD control feature the same should be disabled Switch (config)# no udld enable Switch (config-if)# no udld port Switch (config-if)# udld disabled
Is the scheduler interval/scheduler allocate command used to prevent ssl flooding attacks?	o	ý		The following commands can be used to guarantee processor time to the processes Switch(config)#scheduler interval 500 Switch(config)#scheduler allocate 4000 400
Is ICMP redirects disabled on the switch?	o	ý		The following command is used to disable the service Switch(config-if)#no ip redirects Switch(config-if)#no ip unreachables Switch(config-if)#no ip mask-reply
Password Encryption				
Are the passwords viewable when displaying the switch configuration?	ý	o		Passwords should appear encrypted when viewed. The following command is used to implement the same Switch(config)#service password-encryption
Authentication Settings				
Is the enable secret password command used on the switch?	ý	o		The enable secret command should be disabled to implement MD5 hashed password on enable mode Switch(config)#enable secret password
Does the enable secret password match any other username/telnet password			The enable secret as well as the telnet	The enable secret password should be

enable password or the enable secret password of another switch?	o	ý	password is different across each switch	unique across each switch and should not match the telnet console password
Is a login banner defined on the switch discouraging unauthorized users to try to telnet into the switch?	o	ý		Login banners should be used as a preventive measure against unauthorized access to the switches Use the follow ng command to enable a login manner Sw tch(config)#banner motd An exec-timeout should be defined to prevent an attacker from hijacking sessions
Is the following defined on the console port Exec-timeout (Yes/No) Duration of timeout Password Un ques accounts access ng the port	ý	o		Passwords assigned to console ports should be unique from the rest of the passwords assigned to systems Use the following command Sw tch(conf g)#l ne con 0 Switch(config line)#exec-timeout 5 0 Sw tch(conf g line)#password password The aux port should be disabled An exec-timeout should be defined to prevent an attacker from hijacking sessions
Is the aux port disabled?	y	o		
Is the following defined on the vty lines Exec-timeout (Yes/No) Duration of timeout Password Priv lege Level	ý	o	Although a password is defined an exec-timeout is not defined on the vty lines	Passwords assigned to console ports should be un que from the rest of the passwords assigned to systems Use the follow ng command to ass gn an exec-timeout for the vty lines Switch(config line)#exec-timeout 5 0
Is the vty lines restricted to certain IP Addresses only?	o	ý	Vty lines are not restricted to specific lines	vty lines should be restricted to certain IP Addresses only
According to policy, how often do switch passwords have to be changed?	o	ý	Not yet defined nor practiced	The same should be brought into practice
How often is the telnet password changed?	o	ý	Not yet defined nor practiced	The same should be brought into practice
Do the switch passwords meet with the required complexity as defined by the policy?	y	o		
Is SSH/Telnet used for the vty lines?			Telnet is used to manage the switches	SSH is a preferred protocol over Telnet for vty access
Is an OTP system used along with the telnet/ssh process? (One Time Passwords-OTP)	o	ý	To have the strong authentication before grating access it is recommended to be implemented for all the critical IT resources.	
Do any management applications use telnet to perform management activities such as backing up configuration?	o	ý	As it is unsecured it should not be used	Telnet is clear text communication and it is not recommended to use the same
Setting up Usernames Are any local usernames configured on the sw tch?	y	o	There is no 3rd Authentication server used	
Is TACACS+/RADIUS access configured to the sw tch?	o	ý	Not Applicable	Not Applicable
Is there a documented procedure for creation of users on the switch?	o	ý	Not applicable since a common password is used by single Admin	A documented procedure for creation of users on the switch should exist
Does each switch administrator have a unique account for himself/herself?	o	ý		Each switch administrator should have a unique account for himself / herself to maintain accountability
How many exec levels have been defined on the switch?			Default	Default
Which of the follow ng lines are configured through TACACS+/RADIUS Vty lines Console port			Not Applicable	Not Applicable
Is log n and logout track ng for the switch administrators through the TACACS+ system enabled?	o	ý	Not Applicable	Not Applicable
Is command logging enabled for the switch admin strators/users?	o	ý	It should be enabled	As a part of best practice the same should be enabled
Are all user accounts assigned the lowest priv lege level that allows them to perform their duties? (Principle of Least Priv lege) Management Access	o	ý	Not applicable	All user accounts should be assigned the lowest privilege level that allows them to perform their duties
Is the HTTP Server used for switch management?	o	ý		The http service transmits data in the clear text and is hence not recommended The following command can be used to disable the same Switch(config)#no ip http server Typically SNMP vers on 3 should be used on the switch If SNMP v1 or v2c is used security

				measures such as ACL s on the SNMP process should be implemented
Which version of SNMP is used to manage the switch?	o	ý	SNMP is not used to manage the switch	If SNMP is not used on the switch disable is completely using the following set of commands Switch(config)#no snmp-server community Switch(config)#no snmp-server enable traps Switch(config)#no snmp-server system shutdown Switch(config)#no snmp-server
Is the SNMP process restricted to certain range of IP Addresses only?	o	o	Not applicable	Not Applicable
How often is the SNMP community string changed?	o	o	Not applicable	Not Applicable
Is the default community strings such as 'public' and 'private' changed?	o	ý	Not Applicable	Default community strings such as 'public' and 'private' should not be used
Do any of the management applications use SNMP to manage the switch?				
If yes, specify which ones have read-only access and which ones have read-write?	o	ý	Not Applicable	Not Applicable
Is CDP disabled on the switch?	o	ý		CDP should be disabled on the switch if not used by any application Switch(config)#no cdp run
Is logging enabled on the switch?	o	ý		Use the following command to enable logging Switch(config)#logging on Switch(config)#logging host ip Switch(config)#logging trap informational
Which application is used to collect the log messages?				
In which network is the application/syslog collector residing? (mention subnet)	o	ý	Not applicable	Not Applicable
What is the logging trap level defined?	o	ý	Not applicable	Not Applicable
Is any access list defined restricting the syslog host to receive log messages from the switches only and only administrators' systems to connect to the log host?	o	ý	Not applicable	Not Applicable
Is a NTP server used to synchronize the clock of the switch?	ý	o	The same has been implemented	The NTP service helps to synchronize clocks between networking devices and maintain a consistent time
Is a separate logical or physical network used to manage the switch?	o	ý	It is recommended	Switches should be managed using a separate physical network or by creating a separate VLAN
Security				
Is VLAN 1 used for in-band/out-of-band management traffic?	ý	o		
Is the management VLAN configured on any trunk or access port that doesn't require it?	o	ý		Management VLAN's should not be trunked
Is VLAN 1 used for user or trunk ports?	ý	o		VLAN 1 should not contain any user ports or trunk ports
Is PVLAN used for layer2 separation for servers?	o	ý		
Is VTP enabled?	ý	o		
Is the Enable VTP passwords to authenticate VTP advertisements enabled?	o	o	Not Applicable	Not Applicable
Is vtp set to 'transparent mode'?	o	o	Not Applicable	Not Applicable
Is Dynamic Trunking Protocol enabled on the switch?	o	o	Not applicable	Not Applicable
Are non-trunking interfaces in permanent non-trunking mode without negotiation?	o	o	Not applicable	Not Applicable
Are trunking interfaces in permanent trunking mode without negotiation?	o	o	Not applicable	Not Applicable
Are all VLANs that are part of the trunk listed?	o	o	Not applicable	Not Applicable
Is a unique native VLAN defined for each trunk on a switch?	o	o	Not applicable	Not Applicable
Is the Spanning Tree Protocol attack mitigation through the use of BPDU Guard, Root Guard enabled?	o	o	Not applicable	CatOS> set spantree portfast bpdu-guard enable IOS(config)#spanning-tree portfast bpduguard CatOS> set spantree guard root 1/1 IOS(config-if)#spanning-tree guard root (or rootguard)

Is port security enabled on the switch?	o	ý		Use the following commands to enable port security on the switch Switch(config)#switchport port-security mac-address mac-address
Logistics for Configuration Loading and Maintenance				
What switch information is backed up and where are the backup switch configurations stored?	ý	o	The switch configuration is backed up This copy is backed up on the Laptop and on repository server	
Is the backup moved to an off-site/DR site?	o	ý	It should be part of BCP practices	Backup copies should be maintained on site for quick recovery as well as off-site for faster recovery during a disaster
On the system where the configuration files are stored is the local operating system's security mechanisms used for restricting access to the files (i.e password restricted file access)?	o	ý	As it contains the critical information of the company the same should be implemented	
Is TFTP protocol used to transfer configuration or image files to and from the switch? Is the TFTP process restricted to certain addresses only?	n	ý		The TFTP protocol transfers files in clear text and hence is unsafe to use The TFTP process should be restricted to certain addresses only to reduce the risk
Is there a documented procedure for backup of switch configurations as restoration if affected by a disaster?	n	y		There should be a documented procedure addressing backup of switch configurations The restoration of the same should also be addressed in the documentation which can come handy in times of disaster
Switch Change Management				
Are all switch changes and updates documented in a manner suitable for review?	ý	o	It is a part of change management practices	
Are request forms used to aid in recording the audit trail of switch changes requested?	o	ý	Not Applicable	A formal change management procedure should be in place address ng points on a) who initiated the change b) impact analysis e) approval by network owner d) post implementation changes
Is current paper copies of switch configurations maintained in a secure location?	o	ý	The same should be maintained.	As a part of best practice it is recommended
Are only authorized personnel with proper verifiable credentials allowed to request changes to service parameters?	o	ý	The same should be maintained	As a part of best practice it is recommended
Switch Redundancy				
How is the CPU utilization/memory monitored?	o	ý	The CPU and memory utilization is not monitored	
Is there a switch redundancy in cold standby or hot standby?	o	ý		A redundant server in cold standby should be readily available
Are disaster recovery procedures for the switch/network documented and are they tested?	o	ý		Disaster Recovery procedures for the layer 2 switch should be documented and tested
Log monitoring				
Are procedures for reviewing the audit logs documented and followed?	o	ý		
How often is the switch logs (covering adm nistrator access /access control) reviewed?	o	ý	Not done since logging is disabled	
Is the review submitted to a higher authority?	o	ý	It should be done as a part of best practice.	
What is the course of action to be followed if any malicious incident is noticed?	ý	o	Not defined	
Security Updates				
Is the network engineer aware of the latest vulnerabilities that could affect the switch?	n	ý	No	He should register in the site providing the details of the latest vulnerability

Findings & Recommendations

S. No.	Findings Recommendations	Implementation Priority
	Configuration Autoload is not disabled Information passed through the network when configuration autoload is enabled is clear text and can be processed by unauthorized users	High
	VTY lines are not restricted to specific ip address It is recommended to configure the access list to allow specific IP's to access the Switch	High
	Backup of the Switch configuration is stored on Administrator's Laptop The backup of the Switch should be taken on External storage devices and should be kept on-site as well as off-site and should be placed in a safe. If backup is taken on Laptop it is necessary to encrypt the file system of the Laptop to	High

avoid unauthorized access	
Although the TCP UDP small servers bootp cha finger services are disabled by default on recent versions of the switch there is no harm in having these services explicitly disabled	Medium
Information passed through the network when configuration autoload is enabled is clear text and can be processed by unauthorized users The following can be done to disable the feature	
Switch(config)#no service config	Medium
Switch(config)#no boot host	
Switch(config)#no boot network	
Sw tch(config)#no boot system	
Directed broadcast should be disabled on the switch The following command is used to disable the service	Medium
Sw tch(config-if)#no ip d rected-broadcast	
Proxy ARP should be disabled on the switch The following command is used to disable the service	Medium
Sw tch(config-if)#no ip proxy-arp	
To prevent misuse of the Flow control feature the same should be disabled	Medium
Sw tch (config-if)# flowcontrol receive off	
To prevent misuse of the UDLD control feature the same should be disabled Switch (config)# no udld enable	Med um
Sw tch (config-if)# no udld port	
Switch (config-if)# udld disabled	
ICMP red rects should be disabled on the sw tch Thefollow ng commaho is used to disable the serv ce	Medium
Switch(config-if)#no ip redirects	
Sw tch(config-if)#no ip unreachables	
Switch(config-if)#no ip mask reply	
Log in banners should be used as a preventive measure aga nst unauthorized access to the sw tches Use the following command to enable a login hammer Switch(config)#banner motd	Medium
The NTP serv ce helps to synchron ze clocks between networking dev ces and maintain a consistent time	Med um
Logging is not enabled on thn Switch Use the following commannt to enable logging	
Switch(config)#logg ng on	Med um
Switch(config)#logging host ip	
Sw tch(config)#logg ng trap informat onal	
VLAN 1 should not be used for user ports Use another VLAN for example VLAN 2	Medium
Port Security should be enabled on the routers to help mt gate various network attacks	Med um
There should be a documentnt procedure addressing backup of switch configurations The restoration of the same should also be addressed in the documentat on which can come handy in times of disaster	Medium
Disaster recovery procedures for the switch/network should be documentnt ann tested	Medium
Change management procedures should address any changes introduced on the switch	Medium
A redundant switch should be arranged to address its unavailability during a disastar	Low
CDP should be d sabled on the Sw tch To disable CDP use follow ng command Switch(config)#no cdp run	Low
The following commands can be used to guarantee processor time to the processes	
Switch(config)#scheduler interval 500	Low
Switch(config)#scheduler allocate 4000 400	

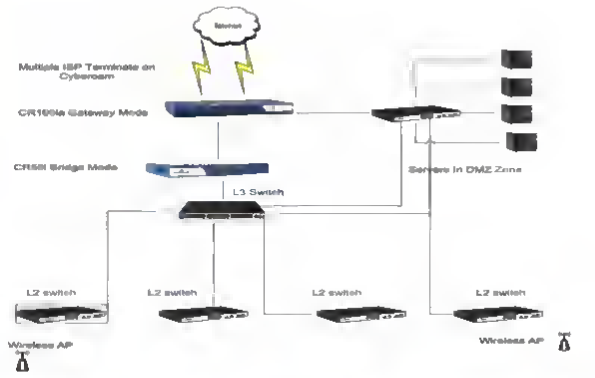
Vulnerability Assessment for IP address

Systems Details			Vulnerability Findings		
Sr No	IP Address	Open Port	High	Medium	Low
1	192.168.100.7	12	0	2	30
2	192.168.100.13	12	0	4	43
3	192.168.100.29	22	1	2	36
4	192.168.100.36	11	5	4	29
5	192.168.100.53	9	1	3	46
6	192.168.100.63	12	1	6	36
7	192.168.100.71	11	0	0	19
8	192.168.100.78	10	0	0	15
9	192.168.100.78	15	6	10	45
10	192.168.100.83	11	1	3	37
11	192.168.100.89	10	1	5	45
12	192.168.100.98	15	3	5	48
13	192.168.100.124	11	1	8	57
14	192.168.100.126	13	5	3	40
15	192.168.101.155	13	0	4	36
16	192.168.101.166	9	0	4	34
17	192.168.101.172	11	3	3	46
18	192.168.102.250	11	0	1	26
19	192.168.102.251	9	0	0	21

Network Architecture Review

Existing Diagram

Suggested Network Diagram



Recommendation

1 As per the existing diagram there are many nodes which are directly connected to Internet without any security which leads entry point for the malicious traffic/threats We recommend gateway level firewall should be at the edge and rest all nodes should be beh nd firewall
2 Servers should be part of DMZ.
3 LAN can be segregated n to different VLANs which will help in administration and applying security policy As you have already security devic available like Cyberoam which helps to scan all inter VLAN traffic.

Web Application Vulnerability Assessment

System Details		Vulnerability Findings			
Sr. No.	Domain Name	High	Medium	Low	Informational
1	Not disclosed	74	75	90	33
2	Not disclosed	7	4	5	13
3	Not disclosed	33	1057	2209	1525
4	Not disclosed	0	30	4	70
5	Not disclosed	0	0	0	1
6	Not disclosed	166	1325	2020	2614
7	Not disclosed	2	65	1005	387

8	Not disclosed	5	1078	1014	94
9	Not disclosed	4	1051	1280	126
10	Not disclosed	0	3	11	21
11	Not disclosed	1	13	1009	17
12	Not disclosed	0	6	2	10
13	Not disclosed	88	44	1002	37
14	Not disclosed	10	3	827	28
15	Not disclosed	5	24	456	1287
16	Not disclosed	182	0	77	3
17	Not disclosed	0	19	1033	40
18	Not disclosed	2	0	3	7
19	Not disclosed	11	1081	1024	6624
20	Not disclosed	1	5	3	5
21	Not disclosed	1002	3	147	764
22	Not disclosed	0	14	340	218

Cyberoam Career Certification

Prepare For CCNSP Certification With The Official Companion Guide

Module 14

Network Forensics

Cyberoam CCNSP

Cyberoam | Learning
academy.cyberoam.com

Supporting a crime investigation

Forensics in Action

Monitoring user activity

In the context of network security it becomes essential for an organization to monitor each activity in the network. For forensics happen. It is required that logging and reporting solution be in place. There are many network transactions that need to be captured and recorded like

- Authentication events
- Email activity
- Messenger/Internet application activity
- Internal Web Server(s) activity
- Web Traffic (HTTP/HTTPS)
- Other Protocol Traffic like FTP etc.

The above points discuss about an organization where there are no restrictions on any user to browse Internet resources, however we are aware that in most of the organizations restrictions do apply. In that case also, a capturing and recording solution is required.

According to a Gartner Survey, for most of the organizations social media should be blocked. The primary reason behind this is loss of productivity. To add more, an organization's own personal information can be leaked and floating on social media. For example, as of current date the popular social networking site Facebook is banned in several countries including Republic of China, Iran, Uzbekistan, Pakistan, Syria and Bangladesh. Additional to this, many bandwidth hungry applications like online music, games, videos..etc. are also banned by organizations.

However, users try bypassing the corporate network with help of a proxy server. Cyberoam application firewall can identify these types of bypassing activities and log them for the network administrator to look upon.

Hence, to conclude, not only the organizations having unrestricted Internet access need to capture and record the network data, but the organizations with strict Internet policies also need it.

Identifying source of data leak

It has majorly been reported by organizations, that their valuable data is leaked because of availability. The motive of data being available to its employees often leads to data leakage. Data leakage source involves two major contributors

- Person/Individual/computer from where the data is leaked
- Media through which the data is leaked

When we talk about a person or an individual leaking the data, it is very difficult to trace down an individual involved in data leakage. Primary reason for the difficulty in tracing is because of the organization's dynamism. To name a few

- Dynamic IP address schema
- Roaming tendency of a user
- Bringing own devices like USB drives, Mobiles..etc. in organization network
- Using own network, example 3G.

An individual who wants to leak the data can do the leak in several possible ways like for example

- Email
- Chat (Messenger)
- Web Upload
- FTP servers
- Cloud Storage Drives
- USB Sticks
- Mobile device memory

Since our scope is limited to network forensics, we shall enhance more on network forensics only, however for the information on cases like USB sticks and mobile device memory, computer forensics comes in handy. We shall also see a sample incident on data leakage in the case study to follow.

Capturing and Recording Data

For a network forensic solution it is essential from the previous explanation to capture and record all the data about "What's going on?" in the network. An efficient forensic solution should be able to capture the following data

- Authentication data along with username in place of IP addresses
- Email transaction data, each small data from an email transaction like sender, receiver, number of bytes, date and time, email subject line, etc.
- Website visit data, each website visited by a user, data like website URL, sub domain, category of website, data upload/download to/from the website, total bytes transferred, etc.
- Messenger data like message sender, receiver, file name, file type, etc.

Not only should the capturing solution be wise enough to record the above data, but it should also consider parameters like storage space and security of captured data. Storage space management techniques have to be employed so that a proper storage space is allotted to the capturing software. Also it should be make sure that all the data is being captured. Like in case of an organization with multiple branches, it has to be ensured that all branch office data is collected and sent to head office. Another point to be noted here

is the safety of data principles like 4-eye authentication must be in place so that the captured data is seen only by authorize personnel

Discovering data

Discovering data is primarily related to filtering the captured data however it is also related to discovering live data like liv connections packet capture traffic discovery and real time traffic logs

A forensic solution must be able to filter data on many criteria s listed in the sub topics below

Email

Filtering criteria should include sender name, sender email, sender IP address receiver name, receiver email, receiving mail serv IP address subject line body text search etc

Chat (Messenger)

Filtering should include username message search file name search file type search file MIME header search etc

Web Upload

Filtering criteria should include username website name URL search category search etc

Analyzing data

Once the capturing recording and discovering of data is done there should be a mechanism where the forensic solution puts th data in proper place meaning in a sensible format which can be easily understood by the investigator The required analysis different in different forensic situation however to shorten it down an investigator's five questions should be answered by th forensic solution namely How? Where? What? When? & Why?

Managing the data

When a forensic solution has loads lo data to manage it should be ensured that proper data management facilities are available T list a few The solution must be able to define the range of dates asking the administrator lo maintain data between a range purg date between a range etc Also it is the task of the solution to maintain proper place and availability on a physical hard disk whe the data will be stored Henceforth we will learn the forensic solution like iView which is available on the appliance like Cyberoa and also as an open-source reporting solution

Understanding Data Recording

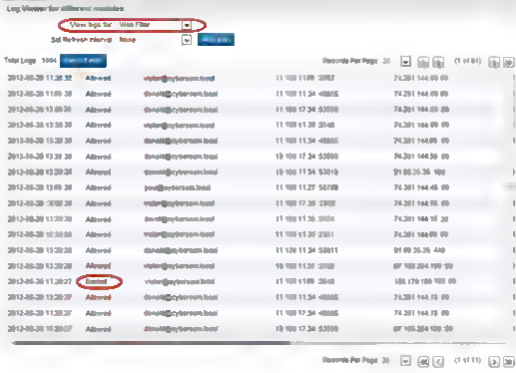
Reporting solution like iView offers a single view of the entire network activity This allows organizations not just to view informatio across hundreds of users applications and protocols it also helps them correlate the information, giving them a comprehensive vie of network activity

With iView organizations receive logs and reports related to intrusions attacks spam and blocked attempts both internal an external enabling them to take rapid action throughout their network anywhere in the world.

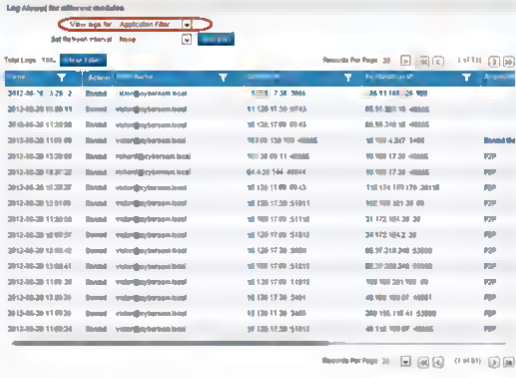
Firewall Captures

The UTM captures are represented on the Log viewer page on the appliance Log Viewer page allows to view the logs for module like IPS Web Filter Anti Spam Anti Virus and Firewall This page gives consolidated information about all the events that hav occurred

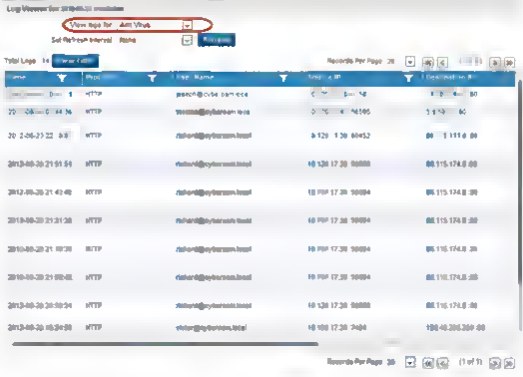
Web filter



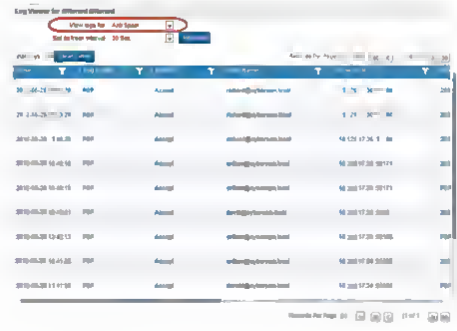
Application Filter



Anti Virus



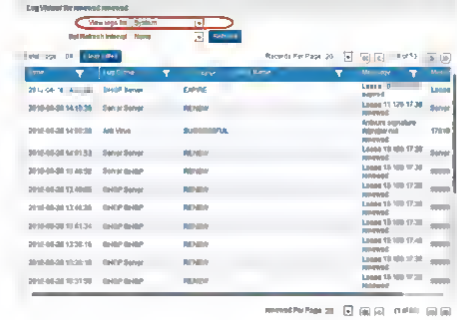
Anti-Spam



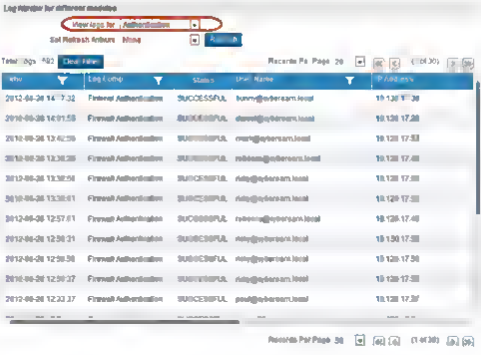
Event Captures

The UTM logs are represented on the Log viewer page on the appliance. Log Viewer page allows to view the logs for modules lik IPS, Web Filter, Anti Spam, Anti Virus and Firewall. This page gives consolidated information about all the events that hav occurred

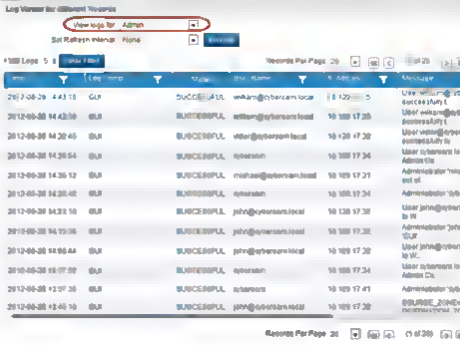
System



Authentication



Admin



Capturing Data

Syslog is an industry standard protocol/method for collecting and forwarding messages from devices to a server running a syslo daemon usually via UDP Port 514. The syslog is a remote computer running a syslog server. Logging to a central syslog serve helps in aggregation of logs and alerts

Appliance can also send a detailed log to an external Syslog server in addition to the standard event log. Appliance Syslog suppo requires an external server running a Syslog daemon on any of the UDP Port

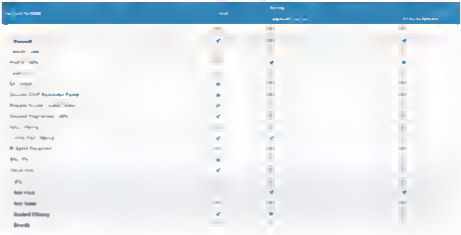
Appliance captures all log activity and includes every connection source and destination IP Address, IP service, and number of byte transferred

A SYSLOG server simply accepts messages, and stores them in files or prints. This form of logging is the best as it provides Central logging facility and a protected long term storage for logs. This is useful both in routine troubleshooting and in incider handling

Firewall Configuration

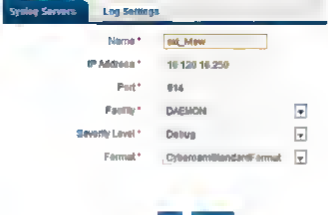
Once you add the server, configure captures to be sent to the syslog server. Go to Logs & Reports -> Configuration -> Log Setting Multiple servers are configured and various logs can be sent on different servers

To record logs you must enable the respective log and specify logging location. Administrator can choose between on-appliance (local) logging, or Syslog logging



SYSLOG configuration

To configure and manage Syslog server, go to Logs & Reports -> Configuration Syslog Servers



Parameters

Name Provide a friendly name for the server

IP Address Provide IP address of the server

Port Provide port number on which CyberoamOS will communicate with the server (Default is 514)

Facility Choose amongst Daemon Kernel Local0-Local7 User

Please Note: More about logging and reporting is described in CCNSE (Expert Certification) as it is beyond the scope of CCNSP to understand the type of facility

Severity Level Choose amongst Emergency Alert, Critical Error Warning Notification Information and Debug

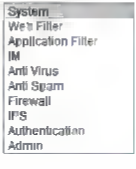
Format: Cyberoam provides logs to the server in CyberoamStandardFormat. On choosing this option the appliance produces log in the specified format.

Viewing Captured Data

Log viewer is a component of the CyberoamOS subsystem It allows viewing logs for modules like IPS Web filter, Application Filter Anti-Spam Anti-Virus Firewall etc It is a page which gives consolidated information about the events that have occurred

To view log viewer navigate to **Logs & Reports -> Log viewer**

Choose from the below options to view logs on that module



Data Analysis

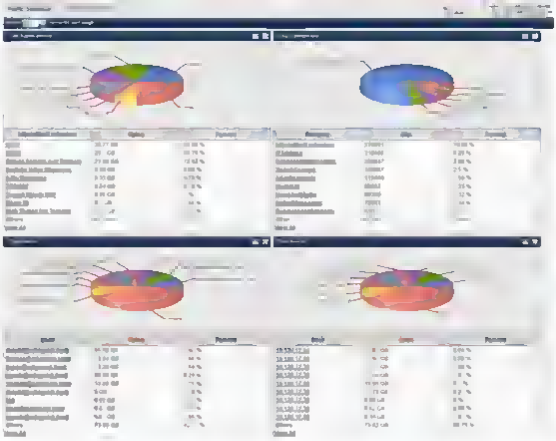
As we already know from the introductory module, Cyberoam appliances come with an on-appliance reporting solution iView Analysis on the recorded data is not only done based on the IP address but also on username as in dynamic environments Identity is the only unique factor Cyberoam iView is a logging and reporting solution which provides organizations with the visibility into the networks to maintain high levels of security and data confidentiality also meeting the requirements of regulatory compliances

Layer 8 analysis

iView not only offers a single view of the entire network activity but also allows organizations to view information across hundreds of thousands of users making it a User based logging and reporting*. With iView in place organizations can receive logs and reports related to intrusions attacks spam and blocked attempts both internal and external, enabling them to take swift action throughout their network being situated anywhere in the globe

View User dashboard

Firewall works at layer 8 and hence the reporting solution also shows the customized and user based reports To see the reports from on-appliance iView navigate to **Logs & Reports -> View Reports** A new window will open the first page on this window is the dashboard giving summary of all the traffic (based on different criteria) To view the user dashboard go to Dashboards -> Custom Dashboard and enter the username for whom you want to view the report

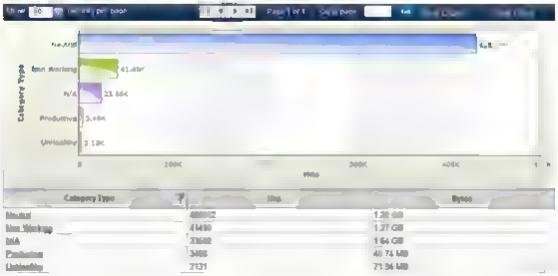


Application Risk Meter

Application Risk meter provides the risk assessment based on the analysis of the traffic through the network. Risk meter is displaye at the top of each page that contains application for an ease to provide an organization with the level of security. By viewing the ri meter, an organization can choose whether to tighten the security or not. The risk meter on iView ranges from 1 5. On this scale 5 high risk 1 s lowest risk. In other words, the lower the number better the security. To mitigate the risks on getting the risk met one can go to the application firewall and check the number of high risk applications that are allowed through the networ Disallowing the potentially high risk applications will bring the application risk meter down and provide best results on the risk meter

Productivity Analysis

Productivity analysis of an organization network can be done from the UTM graphs. iView provides a detailed analysis with graph and stats for an organization to see exactly as to how much productive the use of network is



Blocked Attempts

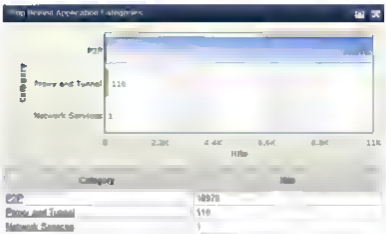
iView generates blocked attempt reports for the web filter and application filter modules. From this report you can view the user trer to try surfing blocked web traffic or trying unhalt blocked applications.

On the blocked application dashboard page, iView shows the following consolidated reports:

To view the blocked attempts go to reports -> Blocked Applications or reports -> Blocked Web Attempts (depending on what repo you want to see)

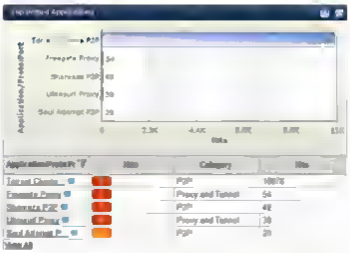
Note Handbook contains explenetion of the deshboard. Each widget on the dashboard is shown separately in the sub topics to follow. In some screens we can find N/A, this is not erroneous, but it means that traffic is being sent to the firewall, without being euthenticeted. In other case, NA can eppear if a IP based rule is defined in the firewall to be denied.

Top denied application categories



The screen above shows the application category which is denied. In this case it is P2P

Top denied applications

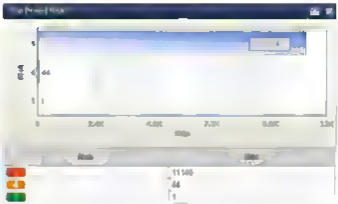


The screen above shows the applications which are denied along with the potential risk they can be (on the risk meter)

Top denied technologies

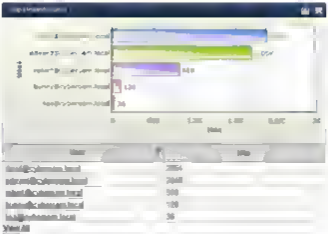
The screen above shows the type of technology used by the denied applications. In this case P2P

Top denied risks



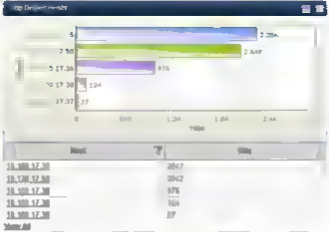
Screen above shows the applications based on their risk level rating (1-5). In this case the applications with high risk (5) are mo used.

Top denied users



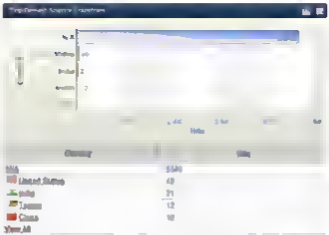
The screen above shows the users who have maximum number of applications denied against their usernames

Top denied hosts



The screen above shows the top denied IP Addresses. This is useful when in dynamic environment, with guest users being allowe to access resources in the network

Top denied source countries



The screen above shows the top denied source countries. In this case N/A appears for a reason that the traffic is between th Internal hosts. In other case, we also see other countries than US primary reason being that some tunneling applicatio randomizing an IP Address was used. This report is created by checking the source IP on each packet that is sent across the Lay 3 firewall

Top denied destination countries

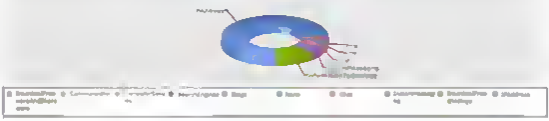
Top denied destination countries shows a general analysis on the kind of traffic flow based on country. From this report a organization can knew the pattern of destination on which their network traffic is hitting. In this network case, maximum traffic hitting India

Top denied rule id

This screen shows the top firewall rule ids through which the applications are being denied. In this case only one firewall rule id (
le denying the application traffic.

Blocked web attempts

This section shows the number of blocked web attempts based on the web category



Top denied web users

The above screen shows top denied users. In this case N/A appears in the following case

A user is not authenticated through Appliance but their browser sends some request. In this case, attempt from the browser
blocked

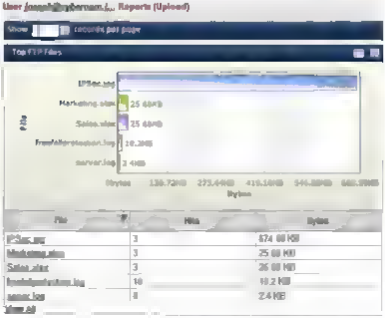
Top denied domains

The above screen shows the top denied domains

Graphical Overview of Data Transfer and Risk Level

Data Leakage

CyberoamOS proactively monitors and reports file uploads which can possibly lead to data breach and leakage. For an organizatio
d is essential not only to maintain the availability of the files of its employees, but also integrity and harmony. For an example
hardware manufacturing company will have to share the component list with employees, but at the same time, it is mandatory th
the design principles, copyrights, and trademarks are not leaked. For this purpose, go to Reports -> FTP Usage -> Top FTP Use
(Upload) or Top FTP Users (Download)



In this case, we can see that the user joseph@cyberoam.local has uploaded 5 files to an FTP server

Searching within data

iView's deep and extensive search algorithm lets you search the reports on multiple and mixed criteria. There are five main types
searches that can be performed on the iView database

- Web Surfing
- Mail Usage
- Spam
- Virus
- FTP

Note. Each of the searches listed above can be found under the Search menu on the left side of the screen

In Web Surfing report search can be done on the following criteria:

- Report Type: Can either be summary or in detail
- Search type: Can be a domain, URL, Category, or an IP Address
- Search for: Can be a User or a Group

Username Specific username

Domain a particular domain name like www.example.com

The detailed report this search can be seen from the screen below

iView allows exporting the reports into multiple formats like MS-Excel & Adobe PDF To export a report into PDF or XLS click on the

required icon to download file directly from the browser

Compliance data

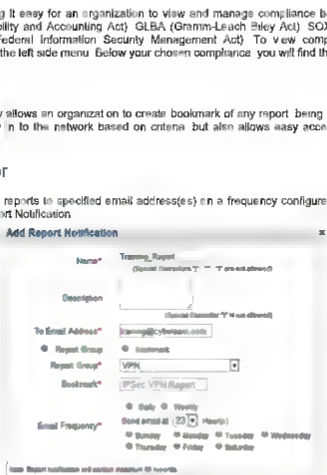
iView is compliant ready making it easy for an organization to view and manage compliance based reports iView is compliant HIPAA(Health Insurance Portability and Accounting Act) GLBA (Gramm-Leach Bliey Act) SOX (Sarbanes-Oxley) PCI (Paymen Card Industry) and FISMA (Federal Information Security Management Act) To view compliance based reports navigate Compliance Reports section on the left side menu Below your chosen compliance you will find the compliance based reports

Bookmarks

Bookmark management in iView allows an organization to create bookmark of any report being at any level It not only provides a organization with wider visibility in to the network based on criteria but also allows easy access to most common and importa reports to an organization

Notifying Administrator

iView if configured to can send reports to specified email address(es) on a frequency configured To use report notifications go System > Configuration > Report Notification



From the above screen all the VPN reports will be emailed daily to training@cybercom.com at 23 00 hours (11 00 PM)

Customize data view

iView being user friendly can be customized as per the requirements of an organization A customized report view will create a

organization's own dashboard report page. In place of default, an organization can customize what content it wants to see when iView loads. For an example, if an organization does not require FTP upload widget on the dashboard, it can be removed and custom widget can be added.

To achieve this, navigate to System -> Custom View

Give a name to the view and an optional description

Note: Dashboard main page has 8 widgets and hence, a maximum of 8 reports can be selected while creating a custom report view

Data Management

CyberoamOS creates different partitions on the disk within appliance such as /root, /Signature, /Configuration, /Reports and /Temp. This can be seen from the disk usage section under System Graphs by navigating System -> Diagnostics -> System Graphs.

	Max	Min	Average	Current
/root	88.00	88.00	88.00	88.00
/Signature	83.00	83.00	83.00	83.00
/Config	88.00	88.00	88.00	88.00
/Reports	81.00	1.00	10.52	1.00
/Temp	78.00	78.00	78.00	78.00

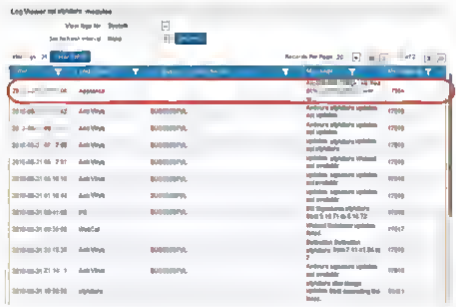
It is essential for administrator to monitor the disk performance and health regularly so as to make sure disk is always under web working conditions. Report partition on the disk takes more place which makes it essential for an administrator to set a watermark (threshold limit) in order to avoid disk usage beyond the defined limit.

Appliance provides Disk Usage Watermark Threshold for monitoring resources. With this when the disk is utilized beyond the configured threshold an alert log is generated in the log viewer. If the disk usage goes beyond the threshold limit define

CyberoamOS will automatically disable on-appliance reporting modules

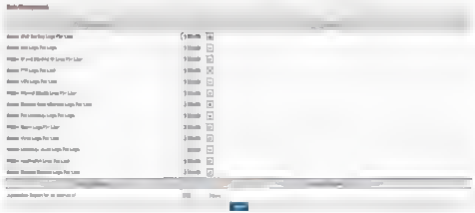
Note The default Threshold limit of the disk is 80%, the higher value (when CyberoamOS will stop reporting) is 90%

For an ease, CLI command can be used to set the lower threshold limit between 60 to 85%
The screen below shows the watermark (threshold) alert in log viewer



Note In the above screen threshold value was set to 60% so as to capture this alert

To manage duration of Data Management for each Module to be retained go to System > Configuration -> Data Management on view



iView also allows a user to manually purge the data go to System -> Configuration -> Manual Purge and choose the duration for which the data is to be purged

On the Cyberoam Console window choose the option 4

```
Main Menu

  1.  Network  Configuration
  2.  System   Configuration
  3.  Route    Configuration
  4.  Cyberoam Console
  5.  Cyberoam Management
  6.  WAN Management
  7.  Shutdown/Reboot Appliance
  0.  Exit

  Select Menu Number [0-7]: 4
```

On the console w ndow type the following command to see the disk currently being used by report partition

```
console> cyberoam diagnostics show disk
Diskname      Size     Used     Avail    Use%
configuration 193.7M   106.0M   87.7M    55%
signature     907.2M   568.4M   338.8M   63%
report        60.0G    792.9M   59.2G    1%
console>
```

To see the watermark level defined for reporting partition key n the follow ng command

```
console> show report-disk-usage watermark
Lower watermark percentage for report partition is 80%
console>
```

Forensic Case Studies

Case Study 1

A XYZ company's ex-employee opens his own company. When found by the XYZ Company, the product has the sam design and same content as manufactured by the ewing company. XYZ Company wants to investigate the networ forensics and find if the design and content data was leaked. If so, XYZ Company already has registered trademarks an copyrights and can claim a lawsuit against the ex-employee. Fortunately, an on device reporting solution UTM lik Cyberoam was installed in the XYZ Company. We shall now see how appliance like Cyberoam helped in solving the networ forensic case.

Before invest gat ng the scenario, the company details have to be known. From the above case study def nition, some of the detai are known, however, to ga n more knowledge about the company, the forensic investigator collects more details about the compan More details from the investigator state that

The company has a total of around 400 + employess

The designing task started around a month earlier and ended on 5th October

Design team comprises of 5 people.

Design team sent the design out to product team

Product team comprises of 10 people, out of which 6 are responsible to work for this product with this design

Initial Investigation

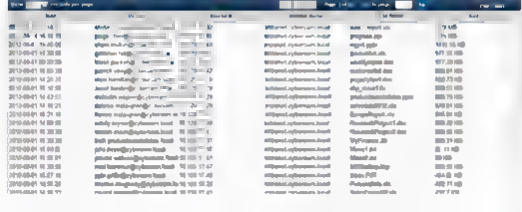
Investigation reveals that 2 people from design team were working on th s design. The des gn was completed on 5th October

Design was sent out using their ema ls to the persons from product team

The leak came into the knowledge of the management on 25th October

Steps involved in this case study

At first we check the web usage for file upload. (Path: Reports -> Web Usage -> Top F le Upload)



File upload report does not highlight any user who has uploaded the design file...hence we now check the email usage with subject line search (Path: Search -> Mail usage)

This reveals that the user "kristina chung"(designer) had sent out the design to 5 people from the product team namely Francis, Sandy, Marion, Beth and Julia

"julia desai" sent the design to jerome wallace, who is no way related to the project.

In the next step, we drill down the usage of Jerome to confirm if Jerome is the suspect

If Jerome leaked the design with help of email, it would have been shown in the previous report itself, but since the design is not in the previous screen we check Jerome's IM usage (path: IM Usage -> Top Protected Contact)

It is revealed from Jerome's IM usage that it was sent out to anthony dcosta using IM

This concludes the case study

Case Study 2

An organization's large file (1 GB) containing essential data and organization business secrets is leaked

From the investigator, the facts known are

The organization has strict policies enforced to its employees since its inception

These polices include...locking USB ports on each computer, all file internet drive applications are locked

Maximum file size supported in email is 25 MB

User's have a monthly quota of 1.5GB. They cannot browse any network resources beyond this limit.

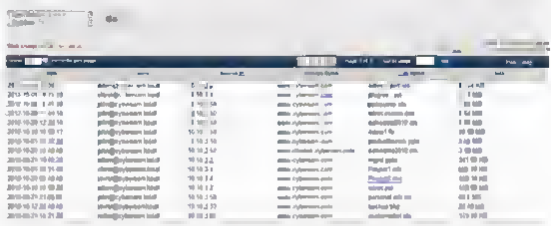
The forensic analysts have been assigned task to find: who leaked the file, and how the file was leaked?

Initial Investigation

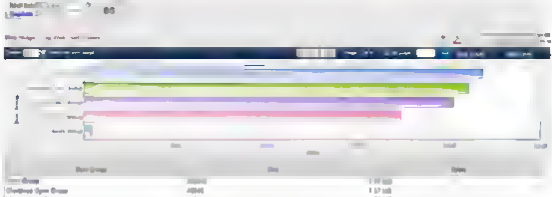
Initial investigation and interrogation with administrators revealed that static IP addresses are assigned to each computer, authentication mechanism are in place, and each user has a quota of 150 MB/day

Steps involved in this case study

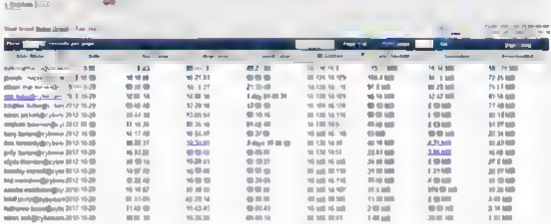
To solve this complicated case, we first drill down the file upload report. (Path: Reports -> Web Usage -> Top File Upload)



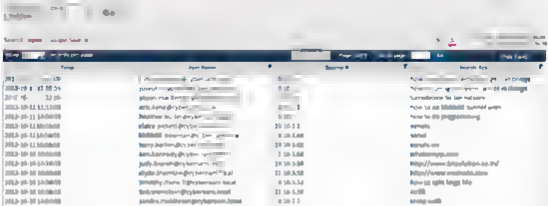
Web file upload does not give any information about a 1 GB file, hence Upon no clues with file upload, we drill down the grou wise web usage report (Path Reports -> Web Usage -> Top Web User Groups). From this screen we shall come to know th group to which the user(who leaked the file) belongs to



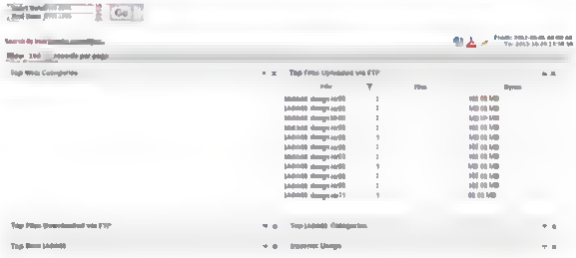
All group usage show the same type of pattern hence it is difficult to suspect any group however we still drill down into th users from each group to see the individual data usage Drilling down nte details of group wise web usage report for clue (path. Search -> Web Surfing Reports)



This screen also does not show the usage by any particular user, hence we are sure that the file was not uploaded directly a 1 GB file Upon no successful clues we are forced to look into the wed search reports (Path Reports -> Search Engine)



Suspect identified drilling into user based reports for web categories files uploaded files downloaded denied categories viruses and internet usage (Path Dashboard > Custom Dashboard)



Suspect confirmed The file was broken down into chunks and uploaded on an FTP server in a span of 11 days

Summary

In this module we have learnt how iView can help deal with forensics analysis iView can re-generate event to help administrator g
into details of each event that occurred in an organization Apart from these we have also enlightened logging & reporting with

- UTM Logs
- Event Logs
- Configuring SYSLOG server
- On-appliance Reporting
- Blocked Attempts
- Compliance report ng
- Bookmarks
- Customize reports

Labs

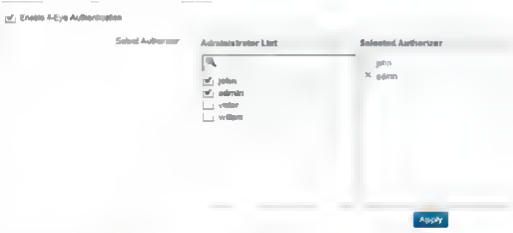
Lab 71 - Configure 4-eye authentication

4-Eye authentication is used when a network can be claimed as a zero trust network. After all the modules that we have studied, we know that the network admin can define and set policies and has the view of all the user data. However, in a zero trust network, if network admin cannot be trusted, we can configure 4-eye authentication.

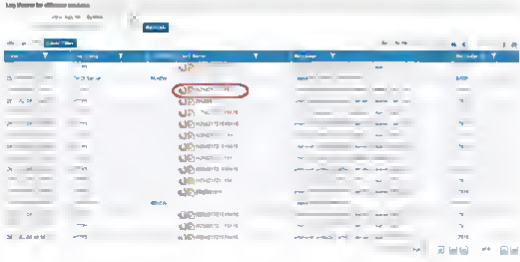
4-Eye authentication requires a de-anonymizer (person who is needed with the network admin) to show an individual's data. 4-Eye authentication will hide all the type of individual data that can lead to a person's identity like IP Address, Username, etc.

To configure 4-Eye authentication, go to Logs & Reports > 4-Eye Authentication and enable 4-Eye authentication.

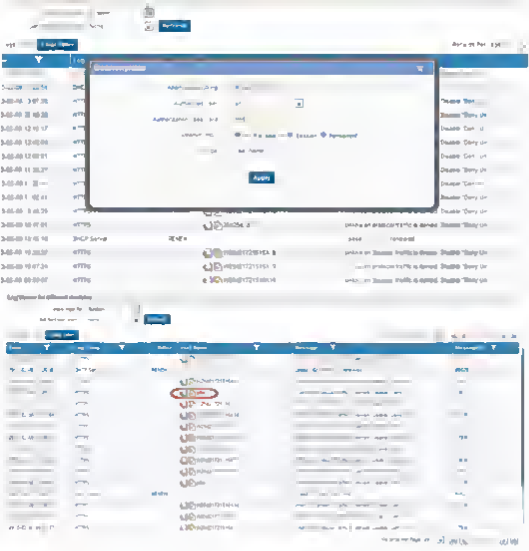
Choose the authenticator (the person who can de-anonymize)



From now, all the reports that can carry an individual's information will be encrypted



To un-encrypt this, we will need de-anonymizer

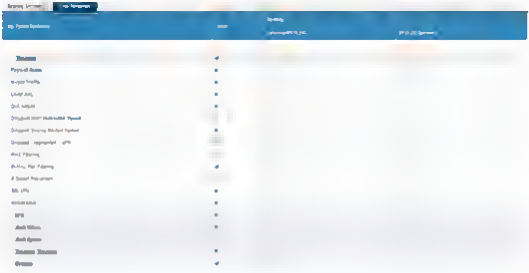


Lab 72- Configure logging & Reporting tool to get maximum data for forensics

To configure logging & reporting module to collect data go to Logs & Reports -> Configuration -> log settings

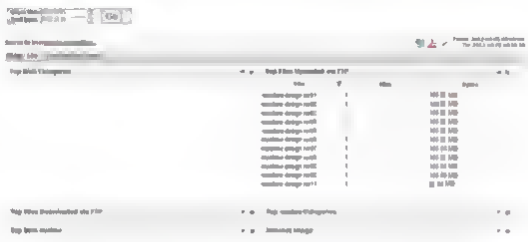
If there are any SYSLOG Servers configured the system will show them in the columns. Each module of the firewall will be listed and its sub features will be listed bellow. Click for eg. Firewall module allows logging of Firewall rules, invalid traffic, Local ACLs, Dos Attacks, Dropped ICP Redirect Packet, etc

Based on the requirement select the required modules click "Apply" and check the reports



Lab 73- generate FTP Data transaction report with File Name for a specific user

To see the FTP data transaction go to Logs & Reports -> View Reports in the new window that opens go to reports -> FTP Usage and select the start date and end date. Based on the data transfer a report will be shown in the format as below



See more reports based on web usage mail usage etc as a part of self activity

Lab 74: Check and report average risk of traffic received from a country

Go to Logs & Reports -> View Reports In the new window that opens, go to reports -> Application -> Top source countries. Click o the country name and see the application risk meter The first screen below shows the list of countries second screen shows th country detailed report.

The risk here is 3.76 based on a scale of 1-5

Lab 75. Check in Real Time what Websites are being accessed?

To check the websites being accessed in real time go to Logs & Reports > Log viewer and select the web filter
This will show the webs tes being browsed currently by the users passing their traffic via Cyberoam.

Certification Pre-requisites

You are now one step closer to being Cyberoam Certified however being Cyberoam Certified requires you to have knowledge about Cyberoam Family Products The below explanation will help you understand Cyberoam better

Next Generation UTM: Cyberoam

The next generation UTM also coined as Identity based UTM appliances are the next generation security solutions While the UTM can only identify the IP addresses Identity based UTM s provide discrete identity information of each user in the network. A better appliance would be the one which has an on-appliance reporting solution The strength of UTM technology is that it is designed to offer comprehensive security while keeping security easy to manage An organization will get complete network information in hand to take any action against a network threat in case any inappropriate activity or behavior is detected in the network

Cyberoam's Security Approach · Overview

Who do you give access to An IP Address, a User...or a MAC Address?
Whom do you wish to assign security policies?
Usernames IP Addresses or MAC Addresses?
In case of an Insider attempted breach whom do you wish to see User Name or IP Address?
How do you create network address based policies in a DHCP and a WiFi network?
How do you create network address based policies for shared desktops?

Layer 8 Identity based Firewall

LAYER 1 to 7 Traditional Firewall

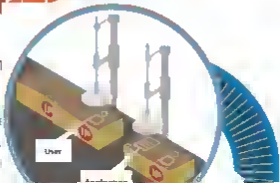
Layer 8 – Patent Pending Tech

Identity Based Security Patent Pending Te

Cyberoam is the only UTM that embeds user

ntent visibility and proactiv

controls over security breaches It offers LDAP,



Protection against Insider Threats

Cyberoam's identity-based security offers prote well as indiscriminate surfin that leave the network vulnerable to external th

Eliminates Dependence on IP Address

Unlike traditional firewalls Cyberoam's identity tify the user. This empowe administrators to control user access irrespective of login IP

Complete Security in Dynamic IP Environments

Cyberoam provides complete security in dynamic IP environments like DHCP and Wi-Fi where the user cannot be identified throug IP addresses. Ilke for example, CEO of the company is a part of each group in the organization and will always wish to be connecte to their company at any location.

One Step Policy Creation

Cyberoam's identity-based security links all the UTM features, providing a single point of entry to effectively apply policies for multip security features. This delivers truly unified control, enhanced ease of use and troubleshooting.

Dynamic Policy Setting

Cyberoam offers a clear view of usage and threat patterns. This offers extreme flexibility in changing security policies dynamically to meet the changing requirements of different

Regulatory Compliance

Through user identification and controls as well as Compliance templates and reports, Cyberoam enables enterprises to mee regulatory compliance and standards. With instant visibility into 'Who is accessing what in the enterprise', Cyberoam helps shorte audit and reporting cycles.

Cyberoam Appliances

Features

Cyberoam offers a well coordinated defense through tightly integrated best-of-breed solutions over a single interface. The result is complete, dependable shield that Internet threats find extremely difficult to penetrate.

- Identity-based Firewall
- VPN integrated with firewall
- SSL VPN
- Gateway Anti-Virus
- Gateway Anti-Spam
- IPS
- HA
- Content Filtering
- Bandwidth Management
- Multi-Link Manager
- On-Appliance Reporting
- 1000+ drilldown reports

WAF (Web Application Firewall)SOHO and ROBO Appliances

Small offices implementing limited security like a firewall and anti-virus leave themselves exposed to high volume and range external and internal threats.

Cyberoam CR15i, CR15wi, CR 25in, CR 35in and CR50in are powerful identity-based network security appliances, delivering comprehensive protection from blended threats that include malware, virus, spam, phishing and pharming attacks. Their unique identity based security protects small office and remote as well as branch office users from internal threats that lead to data theft and loss.

These appliances deliver the complete set of robust security features, including Stateful Inspection Firewall, VPN gateway, Anti-virus and Anti-malware gateway, Anti-Spam, Intrusion Prevention System, Content Filtering, Bandwidth Management and Multi-Link Manager, over a single security appliance.

Small Office Protection

Cyberoam CR15i, CR15wi, CR25i, CR25wi, CR35i and CR35wi offer comprehensive security that is cost-effective and easy to manage, lowering capital and operating expenses for small and home offices. At the same time, these security appliances eliminate the need for technical manpower to configure and manage them.

Remote Office Protection

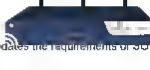
For enterprises with branch and remote offices CR15i CR15w CR25ia CR25wi CR35ia and CR35wi security appliances offer complete visibility into and control over remote users showing "Who is doing what" Given this identity information with user access patterns enterprises can meet regulatory compliances and shorten audit cycles Enterprises can create access policies based on user work profiles enabling them to deploy the same level of security in remote offices that central offices with high security infrastructure and technical resources function in

CR15i – CR15wi

Delivers 3 10/100 Ethernet ports
Configurable internal/DMZ/WAN ports
Supports 30 000 concurrent sessions
With 90 mbps firewall throughput and 15 mbps UTM throughput
CR15wi supports 802 11 b/g/n standards

CR25ia – CR25wi

Configurable internal/DMZ/WAN ports
Supports 130 000 concurrent sessions
Has 4 10/100/1000 Gigabit ports
With 225 mbps firewall throughput and 50 mbps UTM throughput –easily accommodates the requirements of SOHO – ROBO
CR25wi supports 802 11 b/g/n standards



CR35ia – CR35wi

Configurable internal/DMZ/WAN ports
Supports 175 000 concurrent sessions
Has 4 10/100/1000 Gigabit ports
With 500 mbps firewall throughput and 90 mbps UTM throughput –easily accommodates the requirements of small enterprises
CR35wi supports 802 11 b/g/n standards

Cyberoam also have the wireless appliances CR15wi CR25wi and CR35wi which have the same functionality and throughput as mentioned for CR15i CR25ia and CR35ia only difference is they are wireless appliances

Small & Medium Enterprises (SMEs) - Gateway Security Appliance

It isn't true that large enterprises are at greater risk from Internet threats Small and medium enterprises face the same or higher amount of risk from the focused attacks that attackers are shifting to with great success These enterprises need to protect their networks as much as a large enterprise with a large security budget

Cyberoam CR50ia CR100ia CR200 and CR300i are powerful Identity-based unified threat management appliances delivering comprehensive protection to small and medium enterprises (SMEs) with limited investment in financial and technical resources

Cyberoam gateway security appliance offers protection from blended threats that include malware virus spam phishing and pharming attacks at a small business price Their unique identity based security protects enterprises from internal threats that lead to data theft and loss by giving complete visibility into and control over internal users

Comprehensive Security

These gateway security appliances deliver the complete set of robust security features including Stateful Inspection Firewall VPN gateway Anti-virus and Anti malware gateway Anti-Spam Intrusion Prevention System Content Filtering Bandwidth Management and Multiple Link Management over a single security appliance Cyberoam security appliances offer a comprehensive yet cost effective and easy to manage solution that lowers capital and operating expenses in addition to lower technical resource requirement

Regulatory Compliance Through user identification and access control policies for information protection Cyberoam gateway security appliance enables enterprises to meet regulatory compliances like HIPAA, GLBA PCI DSS SOX CIPA and more Further it helps shorten audit and reporting cycles through instant visibility into "Who is accessing what" in the enterprise network

CR50ia

Configurable internal/DMZ/WAN ports
Supports 220 000 concurrent sessions
Has 6 10/100/1000 Gigabit ports
With 750 mbps firewall throughput and 130 mbps UTM throughput

CR100ia

Configurable internal/DMZ/WAN ports

Supports 400 000 concurrent sessions
Has 6 10/100/1000 G gabit ports
With 1 Gbps firewall throughput and 160 mbps UTM throughput

CR200i

Configurable internal/DMZ/WAN ports
Supports 450 000 concurrent sessions
Has 6 10/100/1000 Gigabit ports
With 1500 mbps firewall throughput and 250 mbps UTM th ough ut [illegible]

CR300i

Configurable internal/DMZ/WAN ports
Supports 500 000 concurrent sessions
Has 6 10/100/1000 Gigabit ports
With 1800 mbps firewall throughput and 350 mbps UTM

Large Enterprises : Network Security Appliance

For large enterprises with distributed networks implementing a secure reliable and centrally managed network is critical to deriv trua business benefits Deployment of a range of individual security solutions brings issues of management and control of th solutions particularly at the time of security incident delaying response. In addition with insider threats accounting for 50 % threats identifying the user becomes critical to security

Cyberoam CR1000i and CR1500i are powerful identity-based network security appliances that deliver comprehensive protection large enterprises from blended threats that include malware virus spam phishing and pharming attacks Cyberoam's uniqu ident ty-based Network Security Appliance protects large enterprise users from internal threats that lead to data theft and loss toh

Comprehensive Security

The Check Mark Level 5 certified Cyberoam Network Security Appliance delivers the complete set of robust security features that ar built in order to support the demanding security requirements of a large enterprise Including Stateful Inspection Firewall VPN Gateway Anti-virus and Anti-malware Gateway Anti-Spam Intrusion Prevention System content filtering bandwidth managemen and Multiple Link Management over a single appliance, lowering capital and operating expenses

Cyberoam's Intrusion Prevention System along with stateful inspection firewall gateway Anti-virus and Anti-spyware gateway Ant spam and content filtering offer comprehensive zero-hour protection to enterprises against emerging blended threats

Secure Remote Access

Cyberoam IPSec VPN offers encrypted tunnels for secure communication between remote offices and the central office A unmatched Firewall-VPN performance offers branch offices a secure remote access to corporate resources The VPNC certifie Cyberoam VPN is compatible with most VPN solutions available and supports IPSec, L2TP and PPTP connections It provide automatic failover of VPN connectivity for IPSec and L2TP connections

Enterprise-Class Security

Integrated High Availability feature of CR500ia CR750ia CR1000ia and CR1500ia appliances maximises network uptime an ensures uninterrupted access Cyberoam's Network Security Appliance offers Dynamic Routing that provides rapid optimu increased network throughput with low latencies and trouble-free configuration and supports rapid network growth Cyberoam VLAN capability enables large enterprises to create work profile based policies across distributed networks from a centralise location or head office

CR500ia

Configurable internal/DMZ/WAN ports
Supports 700 000 concurrent sessions
Has 10 10/100/1000 Gigabit ports
With 3Gbps firewall throughput and 750 mbps antivirus throughput caters to the needs of medium-sized enterprises

CR750ia

Configurable internal/DMZ/WAN ports
Supports 300 000 concurrent sessions
Has 14 10/100/1000 Gigabit ports
With 4 5 Gbps firewall throughput and 900 Mbps anti virus throughput [illegible]

CR1000ia

Configurable internal/DMZ/WAN ports
Supports 1 200 000 concurrent sessions

Has 12 10/100/1000 Gigabit ports
Has 4 SFP Mini Ports
With 5 5 Gbps firewall throughput and 1250 Mbps anti-virus throughput caters to the needs of large enterprises

CR1500in

Configurable internal/DMZ/WAN ports
Supports 1 500 000 concurrent sessions
Has 20 10/100/1000 Gigabit ports
Has 4 SFP Mini Ports
With 7 5 Gbps firewall throughput and 1550 Mbps anti-virus [illegible] caters to the needs of large corporate environment educational institutions and government organisations

Features offered with one time sale of appliance and subscription modules

Basic Appliance (One time Sale)

Identity-based Firewall
8 x 5 Support for one month from the registration
VPN - Threat Free Tunnelling
SSL VPN
Bandwidth Management
Multiple Link Management
WAF

Subscription

Gateway Anti-Virus Subscription (Anti malware, phishing, spyware protection included)
Gateway Anti-spam Subscription
Web & Application Filtering Subscription
Intrusion Prevention System (IPS)
8 x 5 support
24 x 7 Premium Support

(Subscription services are available in 1 Year, 2 Year or 3 Year subscription basis)

Bundled Subscription

Bundle can be the combination of or all of the following modules.

Gateway Anti Virus
Gateway Anti-spam
Intrusion Prevention System
Web and Application Filter
8 X 5 Support

Bundle Subscription Types

Bundle Subscriptions are available as

Total Value Subscription (TVS)
Anti Virus
Anti Spam
Web & Application filter
IPS
8*5 Support
Security Value Subscription (SVS)
Anti Virus
Web & Application filter
IPS
8*5 Support

How to subscribe

Upon purchasing the appliance, it is mandatory for a user to register their appliance. The registration can be done by going t

customer.cyberoam.com

Once registered a subscriber has to enter their appliance key in the customer portal

A customer can add more than one appliance to their customer portal

Subscriber will be provided a single key for all the modules included in the bundle

For renewal subscriber can choose to renew the pack or the single module

Each module comes with 3 free trials of 15 days each Trials can be activated by clicking on "Trial" So after registering th appliances customer can use these trail subscriptions before purchasing the subscription keys

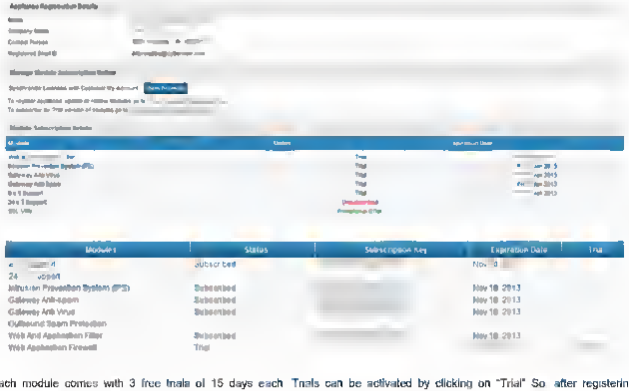
If customer has already purchased the subscription keys he can click on Subscribe and provide the subscription key

Subscriptions can be checked from two places

Cyberoam Appliance (Screen 1)

Customer Portal (Screen 2)

Subscription Screen in Cyberoam appliance



Each module comes with 3 free trials of 15 days each Trials can be activated by clicking on "Trial" So after registering th appliances customer can use these trail subscriptions before purchasing the subscription keys

If customer has already purchased the subscription keys he can click on 'Subscribe' and provide the subscription key

NFR V/S Regular Appliance

Regular Appliance

The Cyberoam appliance sold to Partner / Reseller for direct customer sale Sale appliance can be registered once and can get 3 15 days trials for all subscription based modules

Not for Resale (NFR) Appliance

The Cyberoam appliance sold to Partner / Reseller for conducting end customer demo Demo appliance can be registered unlimite number of times under different credentials after factory reset and can get 3 15 days trial for all subscription based modules aft each registration

CCC (Cyberoam Central Console)

Cyberoam Central Console (CCC) appliances offer the flexibility of hardware CCC appliances and virtual CCC appliances to provic centralized security management across distributed Cyberoam UTM appliances enabling high levels of security for MSSPs ar large enterprises With Layer 8 Identity-based policies and centralized reports and alerts CCC hardware and virtual appliance provide granular security and visibility into remote and branch offices across the globe

Key Highlights

Centralized Management

Cyberoam Central Console (CCC) enables centralized management of updates and security policies in real-time for MSSP managing multiple customer locations and organizations with remote locations minimizing response time. With CCC's Layer identity based policies they can implement role-based access to users offering granular yet flexible controls. CCC allows automatic and manual back-up of Cyberoam UTM configuration including policies and other settings

Security Management with Reduced Policy Deployment Time

With a single web-based GUI across all security features CCC ensures centralized policy implementation simplifying securi management and maintaining high levels of security across all customer locations and remote offices despite the lack of technic resources at these locations. Updations of rules and policies can be centrally scheduled for individual or group of UTM appliances.

Ease and Flexibility of Management

CCC provides flexibility to manage security across various offices and clients by allowing grouping of UTM appliances based on the geography Cyberoam UTM models UTM Firmware versions organizations (especially for MSSPs) and service subscription Enhanced with Web 2.0 benefits the dynamic views in CCC provide at-a-glance information on the dashboard that helps managing searching and sorting appliances by firmware versions appliance models and all appliances. This helps in quic monitoring and action. CCC offers flexibility in sorting appliance views on the dashboard by allowing customizable selection criter for sorting. Email alerts can be set for individual or group of Cyberoam UTM appliances based on parameters like expiry subscription modules excess disk usage IPS and virus threat counts unhealthy surfing hits and more

Security Against Misuse of Administrator Privileges

CCC enables Enterprises and MSSPs to set role-based administration for CCC hardware and virtual appliances as well as individu Cyberoam UTM appliance and group of Cyberoam UTM appliances

Centralized Visibility

CCC's Log Viewer offers logs and views of administrator actions on CCC as well as dispersed UTM appliances which helps investigative analysis supports regulatory compliance as well as keeps track of historical activities across distributed networks

Hardware CCC

CCC 15
- Has 6 10/100/1000 Gigabit ports
- Has 2 USB ports
- Supports up to 15 Cyberoam Appliances

CCC 50
- Has 6 10/100/1000 Gigabit ports
- Has 2 USB ports
- Supports up to 50 Cyberoam Appliances

CCC 100
- Has 6 10/100/1000 Gigabit ports
- Has 2 USB ports
- Supports up to 100 Cyberoam Appliances

CCC 200
- Has 6 10/100/1000 Gigabit ports
- Has 2 USB ports
- Supports up to 200 Cyberoam Appliances

CCC 500
- Has 6 10/100/1000 Gigabit ports
- Has 2 USB ports
- Supports up to 500 Cyberoam Appliances

CCC 1000
- Has 6 10/100/1000 Gigabit ports
- Has 2 USB ports
- Supports up to 1000 Cyberoam Appliances

Virtual CCC

Virtual CCC is available in two versions i.e. as a VMware based server environment and VMware based workstation environmer Virtual CCC model can be predicted from the network size the number of Cyberoam appliances operating currently and taking in

account the future propositions If any customer has opted for VCCC 15 and needs to manage more than 15 appliances a highe model can be reinstalled Each VCCC model has a 5 appliance limit on act vation. On purchas ng a license the max mum number stated appliances can be managed from the VCCC VCCC does not allow purchasing licenses for specific number of appliance other then listed This means on e VCCC 15 you cannot activate 6 7 8 10 or 12 appliance license VCCC comes with forward ar backward compatibility which means that a user on VCCC 50 can transfer the policies to any lower or higher model of the appliance Virtual CCC can be downloaded from http://download.cyberoam.com/virtualccc

Model range

VCCC is available as

CCC VMS 15 CCC VMS 50 CCC VMS 100 CCC VMS 200 for VMware server based virtual environment

CCC VMW 15 CCC VMW 50 CCC VMW 100 CCC VMW 200 for VMware workstation based v rtual env ronment

CCMS (Cyberoam on Cloud Management Service)

CCMS is SaaS (Software as a Service) based In general form it is used for partners and MSSPs to provide value added services their customers CCMS is a free service for active partners To get enrolled for CCMS a partner has to send request to region sales manager and wait for the approval process A partner already enrolled can invite their customers to enrol upon which th partner can manage the services and the Cyberoam appliance CCMS does not allow the distributor to view or manage e partner chatomers appliance unless stated and agreed otherwise

Cyberoam iView

Cyberoam iView is an open source logging and reporting solution that helps organizations monitor their networks across multip devices for high levels of security data confidential ty wh le meeting the requirements of regulatory compliance

Enabling centralized reporting from multiple devices across geographical locations Cyberoam iView offers a s ngle view of the entir network act vity Th s allows organizat ons not just to view informat on across hundreds of users applicat ons and protocols it als helps them correlate the information giving them a comprehens ve view of network activ ty

Monitoring Security

W th Cyberoam V ew organizations receive logs and reports related to intrusions attacks spam and blocked attempts both intern and external..enabling them to take rapid action throughout the r network anywhere in the world

Identity-based Reports

Cyberoam iView offers reports based on the user identity allowing organizations to see "Who is do ng What" anywhere in th network G ven the cr t cal ty of insider threats in network security and data confidential ty these reports give an instant v ew of a use profile through in depth user dentity-based reporting across applications protocols and multiple dev ces and solutions allow m organizations to take preventive measures

Regulat ry Compliance

Cyberoam iViews user identity-based drill down reports form a critical element in enabling organizations to meet the access contro audit and forensic requirements of regulatory compliances like HIPAA GLBA SOX PCI-DSS CIPA BECTA and others

Log Management

The highly connected world changing Internet threat scenario advent of social networking and new business technologies make imperative for organizations to add advanced security solutions and devices like firewalls content filtering systems unified threa management solutions routers servers applications operating systems and more in their networks which generate a vast amoun of log data

To maintain security data confidentiality and meet the requirements of regulatory compliance continuous log monitoring become essential allow ng administrators to interpret unusual events and respond in real time But a comprehens ve analysis of network log becomes a difficult and time-consum ng task w th multiple dev ces leading to multiple management systems and proprieta technologies that del ver logs in different formats.

Cyberoam iView – One-Stop Log Management

Cyberoam iView is an open source logging and reporting solut on that enables organizat ons especially SMEs with tight budgets an limited techn cal personnel to manage logs effortlessly and in near real-time reducing admin strative complexities involved in th process In addition as an open source solut on it reduces cap tal and operating costs s gn ficantly

Centralized Log Collection Intelligent Storage and Instant Retrieval

Cyberoam iV ew allows quick collection storage and retrieval of log data from multiple devices across geographical locations at central locat on elim nating the need to trade-off between speed of log collection and qu ck retrieval Its powerful Log Collect o Agent aggregates data from multiple sources at remote s tes and forwards it rapidly to the centralized locat on It compresses log s gnificantly reducing storage requ rements and associated costs and archives data for easy and secure recovery

Although log nformat on is critical dur ng emergencies each m nute spent in search and retrieval translates into mill ons of dollars lost revenues for organizations Cyberoam iView offers indexing in archives and easy-search on various parameters allowin practically instant retrieval of the required information across terabytes of log data

Identity with Security Management

Cyberoam V ew enables organizations to match "who should be access ng what" with "who is actually accessing what" Whe integrated with identity based perimeter security devices like firewalls anti-v rus and anti-spam systems content filtering system unified threat management solutions and more it generates logs that give a fingerprint of user activity within the network throng username iView's logging with user identity allows the matching of these details with user rights and privileges easily revealir discrepancies in user activity

Compliance Management

Cyberoam iView helps organizations comply with PCI-DSS HIPAA GLBA and SOX requirements with end less many user reports and rapid search to investigate an incident enabling organizations to demonstrate their compliance capability

Reporting

Cyberoam iView delivers comprehensive and graphical reporting on network traffic security incidents bandwidth usage most use applications and hosts and more allowing easy regulatory compliance resource management and quick incident response It offe centralized reporting of selected or all devices in the network on a single dashboard

Aggregated Reporting

With multiple devices deployed in the network rising threats from insiders and external entities organizations need to look deep and monitor network activities not as isolated incidents which individual logs enable them to do but as comprehensive activity

Data from firewalls content filtering systems unified threat management solutions routers servers applications or operatin systems must be viewed across users in flexible reporting format for in depth actionable view of activity

Cyberoam iView – Integrated Reporting from Multiple Devices

Cyberoam iView s the open source centralized logg ng and report ng solution that provides comprehensive drill-down reports offerin admin strators a clear v ew of activ ty across any dev ce user locat on or activity throughout the organization The graphical repor can be drilled down to the third level of nformat on allow ng administrators to v ew multiple reports on a single page for un nterrupte view of multiple network parameters

The centralized view of events and activity across all devices and applications on iView s single dashboard enhances IT efficienc and security while lowering costs involved Administrators can also prioritize the placement of reports based on organization requirements through the high degree of customization offered by iView

Identity-based Reporting

External threats targeting insiders ignorance as well as insider threats that breach network security and data confidentiality are o the rise Cyberoam iView s detailed drill down reports with a clear view of the user and his / her activity over any device location activity throughout the organization allows administrators to see "Who is doing What" in the network

Knowing a person's activity is not just a matter of viewing reports by the username application or protocol It requires comprehensiv tracking of activ ty via keywords attacks and intrus ons with a combination of user application and protocols available at a cl ck an in the form of drill-down graph cal and tabular reports

Cyberoam iView's user identity-based reports give a clear view of the user's network usage like websites visited time and duration for which the user accessed them sites that were denied access to bandwidth consumed by the user across different protocols and more This information allows administrators to judge the user's activity profile the understanding of which enables them to formulate policies taking preventive action against potential security breaches

Meeting Regulatory Compliance

Access control and auditing form the basis of regulatory compliance requirements across the world Cyberoam iView offers reports that cover user activity accessing critical data including attempts to access data where access is denied to the user as well as data leakage by the user across multiple protocols This allows organizations to meet the requirements of regulatory compliances like HIPAA, GLBA PCI DSS SOX and more

Identity based Reporting

Insiders like current and former employees suppliers and partners cause 53 % of security breaches according to a PriceWaterhouse Coopers global survey 35 % of breaches are of intellectual property theft Hence Identity based Reporting that gives visibility into who is accessing critical network resources the extent of usage and user privileges is a critical element of network security

Cyberoam iView – Identity Monitoring

Cyberoam iView is the open-source logging and reporting solution that shows "who is accessing what" in the network, reports network usage violation of privilege entry of malware or spam that can be traced to users enabling organizations to enhance security levels while meeting the requirements of regulatory compliance

User activity over a range of protocols like HTTP, FTP email IM, P2P and more across different user IDs alerts organizations internal security breaches and their source allowing them to take immediate action

Data Loss Prevention

Identity-based reporting of user access plays a key role in controlling data loss Consider this scenario A user attempts to access sensitive documents in the database server to which he does not have access privilege Firstly Cyberoam iView reports his blocked attempts Secondly if the user attempts access via different client devices administrators would be notified through the reports which gives both the username and the IP address from which the attempts are made Such deviation from normal practice alerts administrators to potential violations and data loss

Consider another scenario where the user tries to access the database server through login ids of other employees from her device Administrators would know such takeover attempts through Cyberoam iView, allowing them to take rapid action

Employees on notice can be monitored and their past records revisited and reports provided to HR or the respective department offering critical information related to the users access practices during the most vulnerable period for sensitive data during the employee life cycle

Security Monitoring

Cyberoam iView provides security reports related to malware download or upload spam received and sent Indicating unsafe practices of users In addition reports of attacks attackers victims applications used by the attacks break-down of attacks by severity top spam recipients senders applications used to send spam as well as of viruses bifurcated into web mail FTP through which viruses entered offer effective security monitoring

Web Usage

Cyberoam iView allows administrators to know when users web usage deviates from acceptable policies based on time of activity and volume of data downloaded or uploaded through web usage reports of users categories domains content web hosts and applications Reports of blocked web attempts offer information related to attempts to compromise user privileges A combination of these web usage reports offers a comprehensive view of user web activity allowing administrators to correct user privileges to enhance productivity and security

Security Management

Complexity of IT environments is rising with the use of multiple network devices applications protocols so is the sophistication of security threats While organizations continue to grapple with the source and form of threats attackers are targeting not just the network itself but also databases servers and employee identities in organizations to reap financial rewards

Discovering the exposed threats that most attackers resort to and correlating them with the causes is essential to maintaining high levels of security This involves logging and analyzing thousands of logs generated through multiple network devices across geographical locations on a continuous basis

Cyberoam iView – Security Reporting

Cyberoam iView is the open source logging and reporting solution that offers a comprehensive security view of an organization on a single screen iView delivers identity based logging and reporting across multiple devices protocols and locations enabling organizations to discover not just the threats but also allows them to correlate these with the who what why where when of each attack

This comprehensive approach enables organizations to understand the historic patterns of activity and hence be alerted to deviations in activity that signals an attack and take the precise action required to prevent or contain the attack. Further it allows them

identify disguised attacks, while eliminating false positives

Security at a Glance

Organizations can instantly locate network attacks, their source and destination through a quick glance at the iView dashboard. Further, Cyberoam iView's drill down reports and identity-based logging/reporting related to traffic denied by firewall, content filter, dropped mail by anti-spam, anti-virus and IPS solutions assists organizations in locating an attack, the source-destination and taking rapid action.

Traffic anomalies like a spike in ICMP traffic or in bandwidth consumption that indicate a DoS attack or spyware infection respectively, emails to suspicious mail addresses are some examples of how Cyberoam-iView enables administrators to identify malicious activity, the source and destination, including the user identity where relevant, reducing the response time to threats.

Audit Trail and Forensics

With full archival and storage of logs, Cyberoam-iView aids in audit trail and forensic analysis offering comprehensive security logging and reporting across multiple devices and geographical locations.

Compliance Reporting and Security Audit

Regulatory compliance has become a priority for organizations, requiring overwhelming effort, time and cost in the form of retrieval and storage of logs and reports from multiple devices. Correlating the vast amount of logs and reports to complete the compliance picture is a complicated and time-consuming task.

At the same time, visibility into who has accessed what and when and audit logs hold the key to compliance efforts. Inability to meet compliance requirements can lead to loss of reputation, legal liability and financial losses.

Cyberoam iView – Compliance Reporting

Cyberoam iView's is an open-source logging and reporting solution that enables organizations to meet the requirements of PCI-DSS, HIPAA, GLBA and SOX.

iView eliminates the complexities in compliance reporting by providing access reports and audit logs that alert the administrator of deviations from security practices, significantly reducing the cost to compliance as well as risk to the organization.

Centralized Security Repository

Cyberoam iView offers near-real time reporting of logs and security events on a single dashboard, which can be drilled down to get the third level of information. One-step access to critical information through multiple reports allows end users to monitor security violations in the network, accelerating incident response and facilitating compliance.

Audit Logs

Cyberoam iView enables organizations to maintain integrity of application controls. Organizations can easily identify system configuration changes made by administrators. Concerned personnel can be alerted regarding unauthorized changes, facilitating quick corrective actions.

Forensic Analysis

Ensuring security is a matter of meeting three requirements – continuously judging security readiness to take corrective actions, preventing a security breach and in the case of a breach happening, that of minimizing legal liability.

Forensics is the security element that enables organizations to meet these three requirements through logs and reports that are captured based on potential breaches and legal requirements. In contrast to routine data capture that merely gives historic visibility, forensic view foresees and meets the real security and legal requirements in organizations.

Cyberoam iView – Forensic Analysis

Cyberoam iView is an open source logging and reporting solution that enables organizations to mine historical data from network events. Organizations can reconstruct the sequence of events that occurred at the time of security breach through iView logs and reports. They can reduce the cost of investigation and analysis and minimize network downtime while gathering historical information with Cyberoam iView.

Reduce Legal Liability

Cyberoam iView enables organizations to prove conformance to compliance requirements and reduce legal liability. Consider a scenario where sensitive data kept in the organization's database server is accessed by a user through a stolen identity.

First and foremost, iView reports and audit logs have the capability of identifying the source of breach depending on the security parameters used by the organization.

Further, it enables the organization to prove that it had complied with the security norms and had taken the necessary security precautions to avoid breach in security. Besides this, the network log reports provide evidence that security was intentionally breached by an insider in an otherwise secure network, providing further proof regarding the organization's security preparedness.

With logs and reports that provide such comprehensive visibility with legal validity, Cyberoam iView helps organizations save

significantly on legal costs.